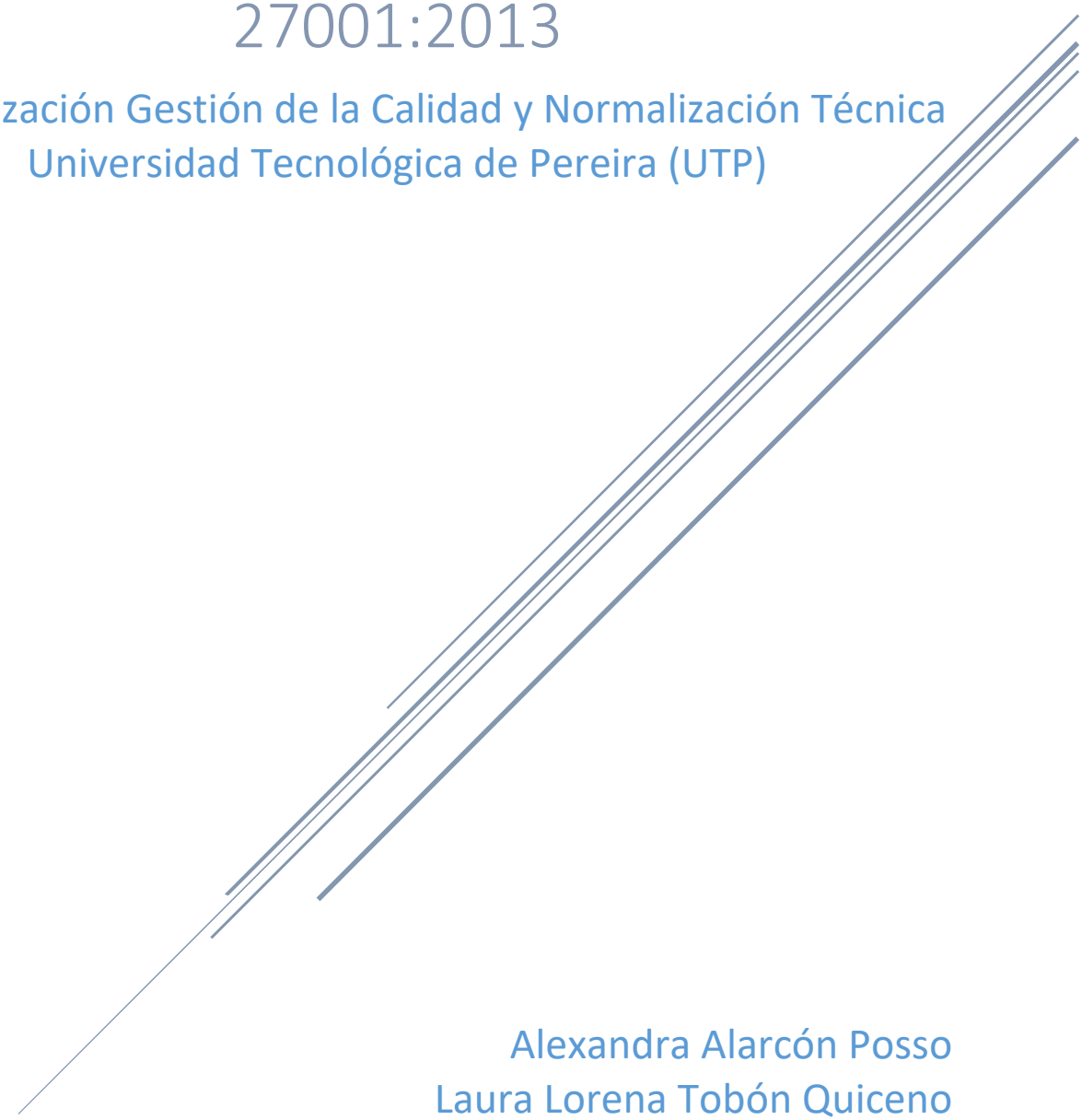
DOCUMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL LABORATORIO CLÍNICO PATOLÓGICO LÓPEZ CORREA BAJO LOS REQUISITOS DE LA NORMA NTC/ISO/IEC 27001:2013

Especialización Gestión de la Calidad y Normalización Técnica
Universidad Tecnológica de Pereira (UTP)



Alexandra Alarcón Posso
Laura Lorena Tobón Quiceno
Pereira, Risaralda

1 DOCUMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL LABORATORIO CLíNICO PATOLÓGICO LÓPEZ CORREA BAJO LOS REQUISITOS DE LA NORMA NTC/ISO/IEC 27001:2013

2 DEFINICIÓN DEL PROBLEMA

2.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad es indispensable destacar la información como un activo importante de las organizaciones, la cual crece exponencialmente, muchas veces sin un control y manejo adecuado. Los Sistemas de Información (SI) son uno de los elementos más importantes en el manejo de la información jugando un papel trascendental en el quehacer diario de las empresas siendo necesario protegerlas de las amenazas internas y externas relacionadas con la información.

Una de las principales falencias de algunas empresas está relacionada con el desconocimiento y la concientización del valor de la información, la cual en ocasiones deja en riesgo su integridad, disponibilidad y confidencialidad exponiendo a la organización a posibles pérdidas económicas y daño a su imagen corporativa. Lo que indica que en algunas empresas existe falta de apoyo de la alta dirección para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) y por ende el posible desconocimiento de la aplicación de las normas de seguridad de la información NTC/ISO/IEC 27001 y 27002.[1]

Se puede identificar varios problemas de protección de la información en algunas empresas por no tener de un Sistema de Gestión de Seguridad de la Información (SGSI) o por una mala aplicación del mismo, además se determinó que el 28% de los casos de robo de información se ejecuta dentro de las mismas, porcentaje significativo, pues su impacto en ellas puede ser fatal, dado que los atacantes internos se pueden considerar delincuentes informáticos. La determinación del nivel de inseguridad (visto desde la óptica de vulnerabilidad y riesgo) de la información trasciende los niveles de su uso u operatividad, de forma que es necesario

[1] Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enriquez Rosero, y Mirian del Carmen Benavides, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001», *Revista Tecnológica - ESPOL* 28, n.º 5 (31 de diciembre de 2015), http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456.

interpretar sus unidades de portabilidad y los medios por los que se transmite, donde se abren nuevas configuraciones al fraude, a la alteración y al uso indebido.[2]

En un ámbito global las empresas deben administrar información que pueda ser accedida de lugares y personas diferentes, generando un riesgo el cual se potencializa porque en su gran mayoría no se cuenta con un responsable del área de gestión de la información, dando como resultado información vulnerable. Los problemas asociados a la seguridad en redes alcanzan a todo tipo de organización, presentándose incidentes y problemas que a futuro vulneran la información. Sumado a esto los empresarios dan poca relevancia al fortalecimiento de los equipos con tecnología de punta y a la toma de conciencia que puedan mejorar los servicios que prestan las empresas. Es importante destacar que en las organizaciones a mayor volumen de información mayor riesgo derivado de pérdidas, alteraciones, manipulaciones o divulgaciones. Estas amenazas causadas por incidentes en la seguridad de la información pueden dar lugar a gastos, pérdida de beneficios o inclusive consecuencias legales.[3],[4]

El Laboratorio Clínico Patológico López Correa presta servicios de especializados en laboratorio clínico, patología, citología y medicina ocupacional, en el cual se maneja información de carácter confidencial, pero no se cuenta con los controles y procedimientos necesarios para asegurar un adecuado tratamiento de la información que permitan mitigar los riesgos asociados a la perdida de la información y a otras posibles amenazas.

De acuerdo a lo analizado anteriormente y con base en los primeros acercamientos realizados al Laboratorio Clínico Patológico López Correa S.A se puede determinar que si bien la información es un activo fundamental para la prestación del servicio y la toma de decisiones, el proceso de sistemas de información debe ser fortalecido desde un enfoque sistémico, teniendo en cuenta entradas, procesos y salidas de la información y además bajo la óptica de la estrategia, diseño, transición, operación y mejora continua. Además de la necesidad de implementar una metodología de

---

[2] Julián Alberto Monsalve-Pulido, Fredy Andrés Aponte-Novoa, y David Fernando Chaves-Tamayo, «InformationVulnerabilities' Study and Management, for a Private Enterprise in the Boyacá ColombianDepartment», *Revista Facultad de Ingeniería* 23, n.º 37 (julio de 2014): 65-72, http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0121-11292014000200007&lng=en&nrm=iso&tlng=es.

3Víctor Daniel Gil Vera y Juan Carlos Gil Vera, «Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas», Scientia et technica 22, n.o 2 (30 de junio de 2017): 193-97, https://doi.org/10.22517/23447214.11371.

[4] Raúl J. Martelo, Jhonny E. Madera, y Andrés D. Betín, «Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)», *Información tecnológica* 26, n.º 2 (2015): 129-34, https://doi.org/10.4067/S0718-07642015000200015.

gestión del riesgo que permita identificar, analizar, controlar y tratar los riesgos potenciales que eventualmente pueden materializarle y vulnerar la integridad, disponibilidad y confidencialidad de la información de la empresa.

El Laboratorio Clínico Patológico López Correa al manejar grandes volúmenes de información en diferentes medios, se ve en la dificultad de implementar políticas y controles eficientes para protegerla de las amenazas que cada vez son mayores y más complejas de detectar, dentro de las cuales están: violación de los niveles de seguridad, para tener el acceso y el control de la información. Colocando en riesgo la integridad, confidencialidad, trazabilidad y disponibilidad de la información, por lo tanto, se hace necesario documentar un Sistema de Gestión de la Seguridad de la Información (SGSI) el cual permita tener un control de la información que es recolectada, producida en todos los procesos del laboratorio, gestionar la seguridad en la operación de los servicios, el soporte de la infraestructura y la provisión de los servicios. Los datos que se poseen actualmente tienen un valor intrínseco, sin embargo, no se dimensiona la utilidad de esa información hasta que dicho valor se descubre.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es la documentación del Sistema de Gestión de la Seguridad de la Información del Laboratorio Clínico Patológico López Correa S.A. bajo los requisitos de la Norma NTC/ISO/IEC 27001:2013?

2.3 SISTEMATIZACIÓN DEL PROBLEMA

1) ¿Cuál es el diagnóstico del servicio de la información actual de la empresa bajo los requisitos de la norma?

2) ¿Cuáles son las diferencias entre el servicio actual y los requisitos de la norma?

3) ¿Cuál es la metodología de gestión del riesgo y como se va a implementar en el sistema de gestión de seguridad de la información de la empresa?

4) ¿Cuál es la documentación requerida en la fase de planeación del Sistema de Gestión de la Seguridad de la Información bajo los requisitos de la norma?

3 JUSTIFICACIÓN

Invertir en la protección la información es un recurso necesario para salvaguardar el valor de las empresas y una forma de hacerlo es por medio de la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basados en la norma NTC/ISO/IEC 27001:2013 la cual da los requerimientos mínimos para la implementación de un SGSI bajo el ciclo PHVA (Planear, Hacer, Verificar y Actuar) incluyendo toda la documentación requerida por la norma la cual es certificable y debe ser renovada cada cinco años. Dicho sistema debe contemplar la normatividad legal vigente y los procesos de análisis y evaluación de riesgos por medio de controles aplicables en forma de políticas y procedimientos alineados con la norma NTC-ISO 27002:2013. El éxito de implementar un SGSI desde cualquier perspectiva empresarial depende del compromiso y la mentalidad de cambio en todos los niveles de la organización, por tanto, el alcance del sistema de información dependerá de un nivel de concientización de las esferas estratégicas y tácticas de la estructura empresarial que conduce a un escenario de competitividad. [5], [6].

En consecuencia el Laboratorio Clínico Patológico López Correa S.A es consciente de la necesidad que tiene de proteger la información, su confidencialidad, integridad, disponibilidad a través de la documentación del Sistema de Gestión de la Seguridad de la Información (SGSI) bajo el cumplimiento de los requisitos de la norma NTC/ISO/IEC 27001:2013 con un enfoque sistémico, alineado con unas políticas claras y controles eficientes, desarrollando e implementando una metodología de gestión del riesgo donde se logrará la identificación, análisis y tratamiento de los mismos, mitigando los riesgos potenciales en la empresa y controlando las amenazas, creando así un ambiente seguro y confiable para todas las partes interesadas, fortaleciendo el proceso de sistema de información y todos los demás procesos que estén intrínsecos en los servicios que se prestan en el laboratorio.

Esto se logrará con el planteamiento de unos objetivos claros iniciando con un diagnóstico del servicio de la información de la empresa frente a los requisitos de la norma, seguido de la identificación de las diferencias entre el servicio actual y los requisitos de la norma, posteriormente con la implementación de la metodología de gestión del riesgo y finalmente cerrar las brechas del Sistema de Gestión de la Seguridad de la Información con la realización de la documentación requerida para darle cumplimiento a la norma en su fase de planeación. Es de resaltar que en la

[5] Yolanda de la N. Cruz-Gavilánez y Carlos J. Martínez-Santander, «ISO / IEC 27001 aseguramiento de la calidad de la información: Línea de tiempo», 2018, https://doi.org/10.23857/pc.v3i6.641.

[6] José Gregorio Arévalo Ascanio, Ramón Armando Bayona Trillos, y DewarWillmer Rico Bautista, «Implantation of a safety managementsysteminformationunderthe ISO 27001: riskanalysisinformation», *Tecnura* 19, n.º 46 (octubre de 2015): 123-34, https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10.

empresa ya se cuenta con la certificación de calidad NTC-ISO 9001:2015 a la cual se le integrará la documentación del sistema de gestión de la seguridad de la información que proporcionará un apoyo importante al momento de realizar la implementación y la futura certificación con la NTC/ISO/IEC 27001:2013.

De acuerdo con lo mencionado anteriormente es importante señalar que la implementación de esta norma incrementa el esfuerzo y el costo, pero gana un camino hacia la mejora y el aprendizaje de las buenas prácticas, al momento de tomar la decisión de implantar nuevos estándares. Pues el enfoque de la ISO está orientado a procesos y tiene elementos comunes en todas las normas y pueden ser integrados con otros sistemas de gestión. El impacto en el corto o mediano plazo en las actividades del negocio da como resultado una reducción de la carga de trabajo y una optimización de las tareas relacionadas con la implementación de procesos, buenas prácticas y el mantenimiento de los sistemas de gestión.[7]

La información cada día tiene una mayor importancia y el conocimiento es el motor de las organizaciones considerándose indispensable con una visión de futuro, la globalización y el desarrollo de la red digital la han convertido en un recurso estratégico clave donde la mayoría de las empresas requieren continuar actuando para elevar la eficiencia de los sistemas de información,[8] protegiéndolos de las amenazas potenciales por medio de mecanismos de gestión basados en las normas internacionales ISO y metodologías de gestión del riesgo idóneas en donde se logrará estandarizar y fortalecer los sistema de información siendo el eje central para el crecimiento organizacional.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Documentar el Sistema de Gestión de la Seguridad de la Información del Laboratorio Clínico Patológico López Correa S.A. bajo los requisitos de la Norma NTC/ISO/IEC 27001:2013 durante el año 2020.

---

[7] Antoni Lluís Mesquida et al., «Integración de Estándares de Gestión de TI mediante MIN-ITs», *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º SPE1 (marzo de 2014): 31-45, https://doi.org/10.4304/risti.e1.31-45.

[8] «Diagnóstico de los sistemas de información en las empresas priorizadas según los requerimientos actuales», 6 de febrero de 2020, http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1853-99122017000100007&lang=es.

4.2 OBJETIVOS ESPECÍFICOS

1) Diagnosticar el servicio de información actual de la empresa frente a los requisitos de la norma.

2) Identificar las diferencias entre el servicio actual y los requisitos de la norma.

3) Definir la metodología de gestión del riesgo e implementarla en el sistema de gestión de seguridad de la información de la empresa.

4) Elaborar la documentación requerida en la fase de planeación del Sistema de Gestión de la Seguridad de la Información bajo los requisitos de la norma.

5 MARCO DE REFERENCIA

5.1 MARCO ANTECEDENTES

En la era de la información es indispensable garantizar la seguridad de los datos e información que reposan en las empresas, protegiéndolas de las amenazas que tanto externa como internamente pueden acarrear contra las vulnerabilidades que allí se presenten, es por esto que se han adoptado medidas de gestión las cuales mitigan los riesgos y permiten además ser más eficientes en los procesos y competitivos en el mercado por medio del diseño e implementación de un Sistema de Gestión de la Seguridad de la Información basados en la norma NTC/ISO/IEC 27001:2013, sentando bases importantes desde la documentación las cuales le dan cumplimiento a los requisitos de la norma.

La información tiene como fin mantener niveles aceptables de riesgo de la información organizacional y de los dispositivos, tecnologías que permiten su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Las normas establecen el deber ser y no la forma como se logra, por eso la importancia de definir metodologías que orienten a las empresas en la forma como se debe abordar este tipo de procesos, con el respaldo de las normas internacionales. La información está relacionada como un activo estratégico de la organización, por lo tanto, las TIC son herramientas que permiten optimizar los procesos de gestión en las organizaciones.

Un Sistema de Gestión de Seguridad de la Información (SGSI) debe proteger la información como recurso valioso, debe proteger de igual forma los diferentes medios a través de los cuales se genera, almacena, procesa, transmite, circula y transforma en un recurso útil para los negocios.
Las fases para la realizar la implementación de un SGSI son:
Fase 1: Aprobación de la Dirección para iniciar el proyecto
Fase 2: Definir el alcance, los límites y la política del SGSI
Fase 3: Análisis de los requisitos de seguridad de la información
Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos
Fase 5: Diseñar el SGSI. [9]

Todas las instituciones independientemente de su tamaño tienen información confidencial la cual debe ser protegida y la forma de garantizar su seguridad según la norma NTC/ISO/IEC 27001:2013 se realiza mediante un proceso sistemático registrado e identificado por la organización que constituye un Sistema de Gestión de la Seguridad de la Información (SGSI). Esta seguridad detecta los puntos débiles que puedan acarrear pérdidas de información suministrando una completa metodología que permite identificar, analizar y administrar los riesgos, valorar los posibles tratos de riesgos y encaminar planes de tratamientos de estos y determinar medidas e indicadores de la eficacia de los controles siendo necesario que existan políticas de seguridad.

Cualquier organización así sea mediana o pequeña puede implementar la norma NTC/ISO/IEC 27001:2013, si tiene como objetivo desarrollar un sistema de gestión el cual garantice la confidencialidad, integridad y disponibilidad de la información. Las pymes aun teniendo clara la importancia que tienen los Sistemas de Gestión de la Seguridad de Información (SGSI) en sus organizaciones prefieren asumir el riesgo de amenazas contra su información a invertir en un sistema que la salvaguarde, sin pensar que esto será un beneficio para el crecimiento que tendrán en el mercado.[10]

Para que una organización permanezca segura dentro de un ambiente de confidencialidad, integridad y disponibilidad de la información es necesario adoptar la visión general que ofrece un Sistema de Gestión de la Seguridad de la Información (SGSI) que se establece, implementa, mantiene y mejora

[9]Francisco Javier Valencia-Duque y Mauricio Orozco-Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000», *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º 22 (junio de 2017): 73-88, https://doi.org/10.17013/risti.22.73-88.
[10]Carlos Roberto Sampedro Guamán et al., «PERCEPCIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN SANTO DOMINGO», s. f., 8.

continuamente mediante el cumplimiento de los requisitos de la norma NTC/ISO/IEC 27001:2013, para que todo activo contemplado dentro del SGSI se mantenga seguro, se proponen controles para mitigar los riesgos que está expuesta la organización evitando así posibles pérdidas económicas o daño a la imagen de la empresa. La inversión a los sistemas de gestión de la seguridad de la información no garantiza la mejora de los resultados empresariales, ya que es necesario que las organizaciones midan los costos y beneficios con la finalidad de conocer la rentabilidad.

Algunos de los principales estándares de la familia NTC-ISO 27000 son:
La NTC-ISO 27001 proporciona un modelo para establecer, implementar, monitorear, revisar, mantener y mejorar un SGSI dentro de cualquier organización bajo el ciclo PHVA (planear, hacer, verificar y actuar) y establece lineamientos para la correcta administración, comprensión y uso de las tecnologías de la información.
La NTC-ISO 27002 establece los lineamientos y principios para implementar, mantener y mejorar la gestión de la seguridad de la información dentro de una organización.
La NTC-ISO 27005 provee directrices para la gestión de los riesgos de la seguridad de la información de acuerdo con la norma NTC-ISO 27001.

A la hora de implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) se debe tener en cuenta el estado actual de la organización y su sistema de gestión de riesgos el cual le permitirá a la alta dirección definir el alcance y aplicación de la norma NTC/ISO/IEC 27001:2013, sus políticas y sus ventajas competitivas que logre mantener la calidad del Sistema de Gestión de la Seguridad de la Información (SGSI) mediante la mejora continua de los controles aplicados.[11]

Con una serie de modelos de evaluación de éxito en donde se pretende explicar la aceptación de las tecnologías de la información de una forma simple y con sustentos teóricos y finalmente la relación de estudios que evalúan el impacto de beneficio que tienen estas tecnologías en el desempeño organizacional y una discusión de los argumentos utilizados para la selección de los factores o indicadores. La calidad de los Sistemas de Información es una medida esencial para su éxito, sus beneficios de aplicación deben contar con indicadores o métricas que en conjunto con el rendimiento del negocio permitan su evaluación y justificación constante. [12]

[11]Oscar Duarte Burgos y Mario Roberto Monges Olmedo, «Análisis de una metodología de Seguridad de la Información basados en los estándares ISO 27001», *Revista ScientiAmericana* 5, n.º 2 (12 de noviembre de 2018), http://www.uamericana.edu.py/revistacientifica/index.php/scientiamericana/article/view/271.
[12]Demian Abrego Almazán et al., «Los Sistemas de Información en el Desempeño Organizacional: Un Marco de Factores Relevantes», *Investigación administrativa* 44, n.º 115 (junio de 2015): 0-0,

El éxito en las empresas para perdurar en el tiempo depende directamente de satisfacer las necesidades del cliente y mantenerse al margen de la competencia por medio del análisis de su entorno en donde las tecnologías de la información y la comunicación (TIC) se han convertido en herramientas no solo de adquisición de tecnología sino también en estrategias competitivas que intervienen en el proceso de toma de decisiones de las empresas como por ejemplo el Sistema de Seguridad de la Información que es una herramienta que se usa para protección de los datos tanto estructurados y no estructurados que provienen de fuentes masivas como el Big Data y el Cloud Computing.

La Norma NTC/ISO/IEC 27001:2013 cuenta con unos aspectos generales sobre la seguridad de la información la cual consiste en la preservación de la confidencialidad, integridad y disponibilidad. En el momento en que se decide implementar dicha norma se deben tener en cuenta las siguientes recomendaciones: Mantener la sencillez y restringir el alcance, gestionar el compromiso y autoridad de la alta dirección, tener un enfoque hacia la certificación como objetivo y apoyarse de otros sistemas de gestión como la NTC-ISO 9001 o NTC-ISO 14001, los cuales se pueden integrar y ser útiles como estructura de trabajo ya que ahorraran tiempo y esfuerzo, se deben registrar todas las evidencias y se debe mantener y mejorar continuamente el Sistema de Gestión de la Seguridad de la Información (SGSI).

La web, los medios sociales y los datos se han convertido junto con las herramientas de inteligencia de negocios en índices de competitividad por ello es necesario la existencia de herramientas que ayuden en la protección de la información proveniente del Big Data y el Cloud Computing, a través de la implementación de un Sistema de Gestión de la Seguridad de la Información que sirva para protegerla. Es importante comprender que además de los datos estructurados (provenientes de fuentes de información conocidas), existen también los datos no estructurados (provenientes de la web, fotos y videos, de las redes sociales, de los sensores de las ciudades y edificios) que presentan una gran dificultad para analizarlos ya sea por la rapidez con la que se generan o por el volumen de contenido que poseen. El Cloud Computing se puede dividir en tres niveles del servicio que son La infraestructura, La plataforma y el software los cuales tienen ventajas en el acceso, sus bajos costos y su espacio de almacenamiento y desventajas en cuanto a la dependencia, la conectividad, el riesgo y la migración[13]

http://www.scielo.org.mx/scielo.php?script=sci_abstract&pid=S2448-76782015000100001&lng=es&nrm=iso&tlng=es.

[13]Ricardo Rafael Coello Yagual y Lucia Magdalena Pico Versoza, «Análisis de las ventajas y desventajas del sistema de gestión dela seguridad de la información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data en el Ecuador», *INNOVA ResearchJournal*, 4 de abril de 2018, 181-95, https://doi.org/10.33890/innova.v3.n4.2018.562.

El papel de las tecnologías de la información (TI) es fundamental para las organizaciones siendo responsabilidad de estas asegurar la confidencialidad, la integridad y la disponibilidad de la información, mitigando el riesgo el cual se encuentra entre las vulnerabilidades y las amenazas de las organizaciones. Cuando se habla de seguridad sobre las tecnologías de información (TI) está enmarcando las siguientes áreas: la seguridad informática (los activos de información), la seguridad de la información (NTC-ISO 27001:2013) y la ciberseguridad (NTC-ISO 27032:2012).

Se contempla de manera general cómo afrontar los eventos adversos de estas áreas bajo la gestión del proceso sistémico, lógico y continuo por medio de un modelo de identificación de los componentes de la seguridad con el entendimiento, explicación y pronóstico del comportamiento de la seguridad y como resultado se observa que los controles juegan un papel indispensable para evitar la materialización del riesgo. Este método de análisis sistémico de los componentes de la seguridad si bien es una propuesta útil ya que cumple el propósito de pronosticar la relación de las amenazas y vulneraciones en un escenario con y sin controles, es un análisis subjetivo pues no hay consideraciones claras. [14]

Debido a la necesidad creciente de cerrar brechas de seguridad que se originan en ataques focalizados al usuario, como por ejemplo a través de trampas de ingeniería social donde todo lo que utiliza el atacante es descartable, genera la percepción de que los atacantes van a un ritmo más acelerado que los defensores, por lo que se hace necesaria enfrentarlas a través de la consecución de políticas de seguridad que impliquen el conocimiento del comportamiento del usuario para su cumplimiento. La mayoría de las organizaciones, tienen políticas de seguridad para proteger la confidencialidad, integridad y disponibilidad de los recursos de información. Las organizaciones desarrollan políticas y procedimientos de seguridad de la información derivados de esas políticas con la intención de mitigar los riesgos operacionales asociados con los muchos usos de los sistemas de información dentro de la empresa.

Los profesionales en seguridad o tecnologías de información, deberían considerar que la seguridad de información no solo se garantiza mediante el empleo de perímetros de seguridad sofisticados, sino que deberían enfocar y considerar en sus estrategias de protección el factor humano, pues dado el comportamiento no deseado que tengan (voluntario o involuntario) provocará la anulación de los

[14]Diego J. Parada et al., «Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas», *Información tecnológica* 29, n.º 1 (febrero de 2018): 27-38, https://doi.org/10.4067/S0718-07642018000100027.

perímetros de seguridad implementados, generando brechas de seguridad importantes, con las consiguientes consecuencias y pérdidas económicas.[15]

Las organizaciones están soportadas, automatizadas y gestionadas por sistemas de información los cuales apoyan a la toma de decisiones, por lo tanto, la seguridad de la información debe ser vista no solo como un accionar defensivo y reactivo sino como un elemento estratégico de la empresa. Las acciones que un sistema de gestión de seguridad de la información busca al ser implantado en una empresa inician con la identificación de los activos de información y finaliza con el análisis, evaluación y tratamiento del riesgo.

El diseño del Sistema de Gestión de la Seguridad de la Información (SGSI) permite determinar los objetivos, procesos y procedimientos para establecer las políticas y controles de la seguridad de la información los cuales serán de gran ayuda para gestionar los riesgos. La metodología empleada para el análisis y evaluación de riesgos con MAGERIT v.3.0 es gratuita y mundialmente reconocida por los organismos de certificación ISO. En el establecimiento del Sistema de Gestión de la Seguridad de la Información (SGSI) se define un comité de gestión del sistema de información, el alcance y la política de seguridad y una metodología de evaluación y análisis de riesgos en la cual se identifican los activos y las amenazas, se evalúa y se le da el tratamiento al riesgo, se seleccionan los controles, se realiza la aprobación para riesgos residuales y la autorización de implementación por la gerencia y finalmente se redacta el enunciado de aplicabilidad.

Se debe tener en cuenta que, junto a la información, el recurso humano es el activo más importante en las organizaciones por lo tanto es necesario que todo el personal, interno o externo, esté debidamente concienciado, capacitado y comprometido con la seguridad de la información. Para esto es primordial crear un comité de seguridad de la información y asignar un representante de este. Y finalmente se concluye que la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) no es un proceso de corto plazo, ya que se requiere de una serie de procesos y requisitos que debe cumplir bajo la norma NTC/ISO/IEC 27001:2013.[16]

[15]JosueRuben Altamirano Yupanqui y Sussy Bayona Oré, «Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento», *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º 25 (diciembre de 2017): 112-34, https://doi.org/10.17013/risti.25.112-134.

[16]Victor Miguel Baca Flores, «DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL - CHICLAYO», *INGENIERÍA: Ciencia, Tecnología e Innovación* 3, n.º 1 (12 de julio de 2016): 42-57, http://revistas.uss.edu.pe/index.php/ING/article/view/357.

La metodología MAGERIT está relacionada con el uso de las tecnologías de la información, es un instrumento que permite la implementación y aplicación de seguridad, genera los principios básicos y requisitos mínimos para la protección de la información. Desde el punto de vista de la gestión de riesgos permite analizar, evaluar, tratar, monitorizar y comunicar los riesgos. La otra metodología analizada CRAMM, está destinada a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y los activos, define el análisis y gestión de riesgos, puede ser aplicable en todo tipo de sistemas y redes de información. Estas metodologías permiten identificar vulnerabilidades, probabilidades, medición y cálculo del riesgo. Inician desde la identificar la información que se quiere proteger, como los activos de información, luego identificar los riesgos y amenazas del entorno para terminar con la definición de mecanismos o controles para reducir el riesgo.

Es importante definir que la seguridad de la información se fundamenta en tres principios; confidencialidad, disponibilidad e integridad. La confidencialidad se refiere a los mecanismos que garantizan el acceso a la información, integridad a la consistencia de la información almacenada y disponibilidad a la característica de que la información esté disponible en el momento de ser requerida. Por lo tanto, la información tiene un valor monetario que por un descuido o por desconocimiento, puede verse comprometida, esto hace referencia al término vulnerabilidad o debilidades que existen en un sistema de información, que permite que pueda ser atacado, evadiendo el control de acceso y la confidencialidad de los datos. Las amenazas son elementos que pueden dañar o alterar la información, y el riesgo es la probabilidad de que una amenaza se materialice y genere un impacto en la organización.

Con el propósito de estandarizar los procesos y actividades para la gestión del riesgo la Organización Internacional para Estandarización, agrupa las mejores prácticas en la familia NTC-ISO 27000 y así administrar un sistema de gestión de seguridad de la información. Por lo tanto MAGERIT, basado en la NTC-ISO 27005 e NTC-ISO 31000, gestiona los riesgos mediante la aplicación de protecciones generales, en claves, en los servicios, en el software, hardware y comunicaciones; CRAMM se alinea al estándar NTC-ISO 27005 en su fase de planificación donde realiza la identificación y evaluación del riesgo.[17]

La gestión de servicios de tecnologías de información (TI), es la gestión de todas las personas, procesos y tecnología que cooperen para asegurar la calidad de vida

[17]Esteban Crespo-Martínez y Geovanna Cordero-Torres, «ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES», *UDAAKADEM*, n.º 1 (2016): 38-47, http://revistas.uazuay.edu.ec/index.php/udaakadem/article/view/129.

de servicios de tecnologías de información (TI), de acuerdo a los niveles de servicio acordados con el cliente. Se basa en funciones tales como sistemas de gestión, gestión de redes, desarrollo de aplicaciones y en los dominios de proceso tales como la gestión del cambio, gestión de nivel de servicio, gestión de problemas, y cuyos principales representantes en el marco de las mejores prácticas son ITIL (InformationTechnologyInfrastructure Library) y la familia de normas ISO (International OrganizationforStandardization) / IEC (International ElectrotechnicalCommission).

En cuanto a la categoría servicios tecnológicos las entidades públicas de la ciudad de Manizales, están calificadas mejor que Pereira y Armenia en cuanto a: Arquitectura de infraestructura tecnológica, procesos de gestión: capacidad, puesta en producción y operación, servicios de administración y operación y soporte técnico y mesa de ayuda, sin embargo, la diferencia es poco significativa.
Por lo tanto, se hace necesario dar cumplimiento de forma más asertiva no solo a los lineamientos normativos establecidos por el gobierno colombiano, sino a las mejores prácticas establecidas en marcos de referencia como ITIL y/o la familia de normas NTC-ISO/IEC 20000.[18]

Existen algunos modelos que permiten el funcionamiento de la gestión de servicios como son COBIT e ITIL con los controles que establece la norma NTC/ISO/IEC 27001:2013. Se aplican a cualquier tipo de organización pública o privada, con servicios centralizados o descentralizados. Para el caso de ITIL, proporciona una descripción del ciclo de vida del servicio, tiene un enfoque basado en procesos, se definen roles y responsabilidades, con el fin de garantizar la calidad de los servicios de tecnología de información y enfocarse en los clientes. Por lo tanto, la Dirección de Tecnologías de Información con respecto a los lineamientos de ITIL, debe realizar la gestión estratégica de los servicios, diseño de los servicios, fase de transición de los servicios, operación de los servicios, gestión y mejora continua.

El COBIT es un conjunto de herramientas de soporte que permite a la Gerencia disminuir las brechas entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Permite a las organizaciones optimizar las inversiones en tecnología, ayuda al diseño de la mesa de servicios y gestionar problemas, incidentes y peticiones del servicio. La NTC-ISO 27000, proporciona un marco de gestión de la seguridad de la información, el objetivo es que las organizaciones puedan garantizar la optimización de riesgo menor para preservar la confidencialidad, integridad y disponibilidad de la información. Incluye las mejores

[18]Carlos Gómez et al., «Las Tecnologías de la Información y las Comunicaciones y los Servicios Tecnológicos en las Entidades Públicas del Triángulo del Café en Colombia», *Información tecnológica* 29, n.º 4 (agosto de 2018): 119-26, https://doi.org/10.4067/S0718-07642018000400119.

prácticas para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de Seguridad de la Información. Las tres metodologías de gestión la implementación de los controles propuestos ayuda a optimizar la gestión de los recursos, minimizar riesgos, mejorar la satisfacción de terceros y la seguridad de la información, alineados con la estrategia y los objetivos estratégicos de la Empresa. [19]

El COBIT 5 integra las mejores prácticas dentro de las cuales está NTC/ISO/IEC 27001:2013 y 27002, el objetivo es identificar los procesos, lo que permite aplicar una mejor práctica, de manera que se mejore el desempeño de la Seguridad de la Información, así definir el alcance y los factores de importancia de los procesos.
Para cada proceso se debe identificar el riesgo inherente, tipo y escenarios de riesgos, el impacto y prioridad a cada riesgo identificado, y así evaluar los riesgos para establecer acciones para minimizar los riesgos. Luego se procede a priorizar los procesos según la importancia y nivel de riesgo. La información que los procesos deben generar o usar para el procesamiento y así identificar las políticas relacionadas con seguridad de la información y las estructuras organizacionales.[20]

No es difícil encontrar problemas de seguridad, un ejemplo es en Chile, el hackeo de las bases de datos personales de 6 millones de chilenos, quedaron disponibles en un sitio público en internet, muestra que la seguridad de la información debe ser resguardada por quienes tienen a cargo esta responsabilidad. El 90% de las Empresas Chilenas son ignorantes en temas de seguridad de la información, 96% son incapaces de detectar un ataque en el sistema y el 99% no posee herramientas para detectar el fraude informático. Tanto los dueños de empresas y ejecutivos no están sensibilizados al respecto reflejado en la poca inversión de sus utilidades en recursos informáticos.

Para contrarrestar esta realidad se deben establecer y mantener acciones que busquen cumplir los siguientes requerimientos: Confidencialidad, integridad, disponibilidad, utilizando modelos como: NTC-ISO 17799, COBIT, ITIL, Ley SOX, COSO, NTC-ISO serie 27000, y así implementar controles de seguridad y políticas claras al respecto, debe abarcar toda la organización y contar con el apoyo de la Dirección para su implementación, e integrarse a las estrategias del negocio, misión

[19]Diana Nathaly López Armendáriz, «Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000», s. f., 19.
[20]«Gobierno de seguridad de la información, un enfoque hacia el cumplimiento regulatorio | Ochoa Arevalo | Revista Tecnológica - ESPOL», accedido 13 de febrero de 2020, http://rte.espol.edu.ec/index.php/tecnologica/article/view/373/258.

y visión con el fin de reconocer su importancia, y así facilitar la formalización y materialización de los compromisos con la organización.[21]

La metodología internacionalmente utilizada en la gestión del riesgo de la información enfocada a las MiPymes llamada ECU@Risk, contempla 4 dominios: Introducción al manejo de riesgos, el marco de gestión de riesgos, el proceso de gestión de riesgos, y recursos. Esta metodología está basada en los principios de la administración de riesgos, provista por los estándares NTC-ISO 31000:2009, y en las mejores prácticas de seguridad de la información: NTC-ISO 27001, NTC-ISO 27002 e NTC-ISO 27005, además del estudio de las principales metodologías internacionales usadas para la gestión de riesgos y seguridad de la información como Magerit V3, Microsoft Risk Management, Octave-S y CRAMM, la proyección a los marcos de referencia COBIT 5 y COSO III, así como también múltiples herramientas de las ciencias administrativas.[22]

Generalmente en las organizaciones independientemente de su tamaño presentan problemas con la seguridad de la información, es por esto que se deben implementar proyectos de gestión para conocer, analizar y mitigar los riesgos asociados a la información y establecer las medidas adecuadas de protección. Adoptando un modelo basado en las normas NTC-ISO 27001 e NTC-ISO 27002 las cuales controlan los procesos de la seguridad garantizando la confidencialidad, integridad y disponibilidad de la información. Cabe mencionar que el 39% de las Pymes y el 52% de las grandes empresas han experimentado daños frente a la seguridad de su información lo que refleja que existe debilidad en los controles de protección.

Se plantea una metodología de gestión de la seguridad de la información de acuerdo a los controles especificados por la norma. Dicha metodología utiliza el ciclo PHVA que busca la mejora continua en los procesos incorporando tres fases de desarrollo que son la planificación, la implementación, la verificación y el monitoreo contemplando los lineamientos de las normas NTC-ISO 27001 y 27002. De acuerdo al juicio de expertos que analizaron este estudio se obtuvo el 73,14% de aceptación de la metodología propuesta, lo que garantiza la coherencia, en su lógica de construcción y funcionalidad.[23]

---

[21]Jorge Burgos Salazar y Pedro G Campos, «Modelo Para Seguridad de la Información en TIC», s. f., 20.

[22]Esteban Crespo Martínez y Esteban Crespo Martínez, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs», *Enfoque UTE* 8 (febrero de 2017): 107-21, https://doi.org/10.29019/enfoqueute.v8n1.140.

[23]Navira Gissela Angulo Murillo et al., «PROPUESTA METODOLÓGICA DE SEGURIDAD DE INFORMACIÓN PARA PROVEEDORES DE SERVICIOS DE INTERNET EN ECUADOR», *Mikarimin. Revista Científica Multidisciplinaria. e-ISSN 2528-7842* 4, n.º 4 (28 de septiembre de 2018): 165-76, http://45.238.216.13/ojs/index.php/mikarimin/article/view/1197.

Los Sistemas de Gestión de Seguridad de la Información finalmente son un mecanismo necesario para las organizaciones que quieran potencializar su seguridad bajo los niveles de confidencialidad, integridad y disponibilidad de la información según los requisitos de la norma NTC/ISO/IEC 27001:2013 la cual tiene como primer resultado ejercer control de documentos y realizar la asignación de actividades para los miembros del grupo de implantación del Sistema de Gestión de Seguridad de la Información (SGSI). Este Sistema de Gestión garantiza el conocimiento, apropiación, gestión y disminución de riesgos de la seguridad de la información para las organizaciones, de forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a cambios que se produzcan en los riesgos, entorno y tecnologías. Por lo tanto, invertir tiempo y dinero en la implementación de un Sistema de Gestión es una decisión correcta para salvaguardar uno de los factores más importantes de las empresas como lo es la información.

5.2 MARCO CONCEPTUAL

5.2.1 Sistemas de Información.

Los Sistemas de Información (SI) son uno de los elementos más relevantes del entorno actual de negocios que ofrece grandes oportunidades para las empresas que aprovechan sus ventajas, pero que a su vez, las impulsa a seguir invirtiendo en este tipo de tecnología, lo que conlleva a la necesidad de medir y examinar sus costos y beneficios, con el propósito de conocer su renta. Lo anterior a partir de una revisión de la literatura.[24]

Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Un sistema de información para la administración: Es un sistema de información basado en computadora, que presenta una colección de personas, procedimientos, bases, tienen como objetivo principal mostrar una visión general de la situación de la empresa. Consecuentemente, estos muestran la situación de las operaciones regulares de la empresa para que los directivos puedan controlar, organizar, planear y dirigir.

Actividades básicas:

[24]Abrego Almazán et al., «Los Sistemas de Información en el Desempeño Organizacional».

a) Entrada de información: Es el proceso mediante el cual el sistema de información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas.

- Las manuales son aquellas que se proporcionan en forma directa por el usuario.
- Las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfaces automáticas.

Las unidades típicas de entrada de datos a las computadoras son las terminales, las cintas magnéticas, las unidades de disco, los códigos de barras, el escáner, la voz, los monitores sensibles al tacto, el teclado y el mouse, entre otras.

b) Almacenamiento de información: A través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. La información suele ser almacenada en estructuras de información denominadas 30 archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros.

c) Procesamiento de información: Es la capacidad del sistema de información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general de un año base.

d) Salida de Información: Es la capacidad de un sistema de información para sacar la información procesada o los datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, discos y la voz, entre otros. Es importante aclarar que la salida de un sistema de información puede constituir la entrada a otro sistema de información o módulo. En este caso, también existe una interface automática de salida. Por ejemplo, el sistema de control de clientes tiene una interface automática de salida con el sistema de contabilidad, ya que genera las pólizas contables con los movimientos de los clientes. [25]

[25]«Sistema de gestión de seguridad de la información en la municipalidad distrital de pira aplicando la norma iso/iec 27001:2013», accedido 2 de marzo de 2020, http://repositorio.uladech.edu.pe/handle/123456789/11988.

5.2.2 NTC/ISO/IEC 27001:2013.

Este estándar internacional nació en 1998 como BS 77779-2 y ahora como NTC/ISO/IEC 27001:2013 el cual se desarrolla como una guía para el análisis, implementación, control y mantenimiento de los Sistemas de Gestión de Seguridad de la Información a través del cumplimiento de sus requisitos pudiendo acceder a la obtención de la certificación internacional. El crecimiento que ha tenido la adopción de esta norma alrededor del mundo es exponencial al pasar en 2006 de tener 5797 certificaciones a tener 27536 en el año 2015 siendo Japón y el Reino Unido los países con mayor número de empresas certificadas.[26],[27]

La norma NTC-ISO 27001 prueba la seguridad de la información y mide la efectividad de un sistema de gestión de la seguridad de la información bajo el ciclo PHVA (Planear- Hacer-Verificar-Actuar) incluyendo toda la documentación requerida por la norma. La familia de la ISO ha evolucionado al pasar del tiempo y de la evolución tecnológica. Desde el año 2005 se adopta la seria 27000 siendo esta norma certificable la más importante de la familia. Para el año 2013 se hace la última actualización hasta la fecha de la NTC-ISO/IEC 27001, la cual está basada en el Anexo SL que es una guía en la cual todos los estándares deben adaptarse a una estructura de alto nivel. Adicional a esto en esta nueva versión de la norma no se establece el ciclo PHVA (Planear- Hacer-Verificar-Actuar) como metodología de mejora continua y no puede ser excluido ningún numeral.

Para la NTC/ISO/IEC 27001:2013 los riesgos deben ser identificados, evaluados y reducirlos a un nivel aceptable por medio de la implementación de mecanismos apropiados, es por esto que esta norma para el tratamiento de riesgos adopta los siguientes pasos: Análisis de riesgos, enfoque de análisis de riesgos, selección e implementación de controles y monitoreo y evaluación de los controles implementados. El funcionamiento de la norma NTC/ISO/IEC 27001:2013 está dado por la gestión de la seguridad de la información en entornos informáticos que prueban la seguridad y miden la efectividad de un Sistema de Gestión de Seguridad de la Información (SGSI) por medio de políticas, procesos y procedimientos que garantizan la seguridad de los activos, la misión, la visión y los objetivos de las organizaciones. De acuerdo con la evolución que han tenido la norma NTC/ISO/IEC 27001:2013 y su importancia que han presentado en el tiempo acarrea

[26]Valencia-Duque y Orozco-Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000».
[27]Vasco Rodrigo Talavera Álvarez, «DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD ESTATAL DE SALUD DE ACUERDO A LA ISO/IEC 27001:2013», s. f., 90.

innumerables beneficios para las organizaciones al salvaguardar la seguridad de su información por medio del desarrollo de un SGSI.[28]

Las organizaciones según la norma NTC/ISO/IEC 27001:2013 deben complementar el ciclo de seguridad en los niveles de confidencialidad, integridad y disponibilidad de la información, constituyendo los denominados Sistemas de Gestión de Seguridad de la Información (SGSI). Al igual que en cualquier otro tipo de organización, la información debe ser adecuadamente protegida es por ello que durante los últimos años, un gran número de empresas se ha interesado por la implantación de la norma NTC/ISO/IEC 27001:2013 como estándar de seguridad de la información y más concretamente, por la implantación de controles de seguridad, definidos en la norma NTC-ISO 27002 (ISO, 2005b) para asegurar o incrementar la confianza de sus clientes respecto de la información que de ellos maneja y proteger los activos propios de la organización para minimizar los posibles daños y asegurar su continuidad.[29], [30]

5.2.3 Sistema de Gestión de Seguridad de la Información (SGSI).

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de responsabilidades, procesos, procedimientos y recursos que establece la alta dirección con el fin de dirigir y controlar la seguridad de los activos de información y asegurar la continuidad de la operatividad de la organización. Los Sistemas de Gestión de Seguridad de la Información (SGSI) nacen como respuesta de las organizaciones a la necesidad de proteger su información crítica del acceso no autorizado o de los daños producidos por la materialización de los riesgos. Los Sistemas de Gestión de Seguridad de la Información (SGSI) contienen la identificación de los activos de la información que deben ser protegidos, los riesgos y las amenazas a los que se encuentran expuestos y los controles que se les apliquen para asegurar la preservación de estos.

El Sistema de Gestión de Seguridad de la Información (SGSI) establece, implementa, monitorea, revisa, mantiene y mejora la seguridad de la información es

---

[28]Yolanda de la N. Cruz-Gavilánez y Carlos J. Martínez-Santander, «ISO / IEC 27001 aseguramiento de la calidad de la información: Línea de tiempo», 2018, https://doi.org/10.23857/pc.v3i6.641.

[29]Julián Alberto Monsalve-Pulido, Fredy Andrés Aponte-Novoa, y David Fernando Chaves-Tamayo, «Information Vulnerabilities' Study and Management, for a Private Enterprise in the Boyacá Colombian Department», *Revista Facultad de Ingeniería* 23, n.º 37 (julio de 2014): 65-72, http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0121-11292014000200007&lng=en&nrm=iso&tlng=es.

[30]Antoni Lluís Mesquida et al., «Integración de Estándares de Gestión de TI mediante MIN-ITs», *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º SPE1 (marzo de 2014): 31-45, https://doi.org/10.4304/risti.e1.31-45.

por esto que es el sistema más importante entre los sistemas de gestión de las organizaciones ya que depende de él salvaguardar la confidencialidad, integridad y disponibilidad de los datos orientado a la gestión y análisis del riesgo. Un Sistema de Gestión de Seguridad de la Información (SGSI) esta soportado en cuatro grandes y continuas etapas para su mantenimiento en el tiempo las cuales son Planear, Hacer, verificar y Actuar (PHVA). Más de 6600 organizaciones de todo el mundo están implementando un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma NTC-ISO 27001 ya que esta norma identifica las amenazas, analiza los riesgos y gestiona la seguridad de la información considerando exigencias en leyes y reglamentos.[31], [32], [33]

Para contrarrestar las amenazas, las organizaciones deben generar un plan de acción frente a estas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación. La definición de SGSI se hace de manera formal y se fundamente en la norma NTC-ISO 27001, donde se recogen los estándares y mejores prácticas de seguridad de la información basado en un enfoque en riesgos. El Sistema de Gestión de Seguridad de la Información (SGSI) está diseñado para asegurar una adecuada selección de controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. Este diseño e implementación está influenciado por las necesidades de los clientes, los objetivos organizacionales, los procesos y procedimientos, por el tamaño y la estructura organizacional y por la complejidad o el volumen de la información. [34],[35]

Para la documentación de los Sistemas de Gestión de la Seguridad de la Información bajo los requisitos de la norma NTC/ISO/IEC 27001:2013 se muestra a continuación las actividades necesarias para darle cumplimiento a estas especificaciones:

[31]«Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos.», accedido 4 de marzo de 2020, http://www.repositorioacademico.usmp.edu.pe/handle/usmp/609.

[32]«Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013», accedido 4 de marzo de 2020, http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6092.

[33]Monsalve-Pulido, Aponte-Novoa, y Chaves-Tamayo, «Information Vulnerabilities' Study and Management, for a Private Enterprise in the Boyacá Colombian Department».

[34]Jorge Burgos Salazar y Pedro G Campos, «Modelo Para Seguridad de la Información en TIC», s. f., 20.

[35]«Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013», accedido 4 de marzo de 2020, http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6045.

- Definición alcance del SGSI
- Definición de una Política de Seguridad
- Definición de una metodología y criterios para el Análisis y Gestión del Riesgo
- Identificación de riesgos
- Evaluación de los posibles tratamientos del riesgo
- Elaboración de una Declaración de Aplicabilidad de controles y requisitos
- Desarrollo de un Plan de Tratamiento de Riesgos
- Definición de métricas e indicadores de la eficiencia de los controles
- Desarrollo de programas de formación y concienciación en seguridad de la información
- Gestión de recursos y operaciones
- Gestión de incidencias
- Elaboración de procedimientos y documentación asociada[36]

5.2.4 Seguridad de la Información.

El amplio uso de las tecnologías de información en los negocios hace que cada vez sea más fácil la expansión de éstos. La comunicación con clientes que se encuentran en una ciudad o país diferente al de ubicación de la empresa, la posibilidad de realizar transacciones comerciales vía web y en general, la facilidad del uso de la tecnología y la globalización de la información para todas las personas ha contribuido a que las organizaciones crezcan cada vez más rápido. Sin embargo, toda esta cercanía y facilidad de uso de la tecnología ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio.

La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización. En la actualidad dado el incremento de la utilización del internet, la evolución de la tecnología y la falta de conocimiento para mitigar riesgos de ataques ha generado innumerables amenazas que aprovechan vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones, ocasionando que se pierdan

[36]Ararat Muñoz y Johanna Carolina, «Diseño de un SGSI basado en la Norma ISO 27001 para la empresa MA PEÑALOSA CÍA. S.A.S. sede principal Cúcuta.», 4 de noviembre de 2018, http://repository.unad.edu.co/handle/10596/21259.

alguna o todas las características que debe preservar la información: disponibilidad, integridad, confidencialidad. [37]

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma que los datos pueden tener: electrónicos, impresos, audio u otras formas. Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. Cabe mencionar que la seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos. [38]

5.2.5 Gestión del Riesgo.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se apoya en estándares internacionales tales como la norma NTC/ISO/IEC 27001:2013. Estos sistemas de gestión utilizan como requisitos, estrategias como el análisis, evaluación y gestión de riesgos dentro del ciclo PHVA (planear, hacer, verificar y actuar), lo que requiere la selección de una metodología sistemática que permita obtener una visión clara y priorizada de los riesgos a los que se enfrenta la organización, identificando los más relevantes y priorizando medidas por implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto, en caso de materializarse. Existen algunas metodologías utilizadas para realizar el análisis de riesgos exigido por la norma NTC/ISO/IEC 27001:2013 en el marco de la implementación de los Sistemas de Gestión de Seguridad de la Información (SGSI), dentro de las cuales están: Octave, Magerit, Mehari, NIST SP 800:30, Coras, Cramm y Ebios.

---

[37]Martha Isabel Ladino A, Paula Andrea Villa S, y Ana María López E, «Fundamentos De Iso 27001 Y Su Aplicación En Las Empresas», *Scientia Et Technica* XVII, n.º 47 (2011): 334-39, https://www.redalyc.org/articulo.oa?id=84921327061.

[38]Campaña Tenesaca y Óscar Eduardo, «Plan de propuesta para la implementación de la norma de seguridad informática ISO 27001 2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP)», noviembre de 2010, http://dspace.ups.edu.ec/handle/123456789/4468.

La norma NTC-ISO 31000 (Estándar sobre principios y directrices para la gestión de riesgo) establece un conjunto de principios básicos que se deben cumplir para que la gestión del riesgo sea eficaz; recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de estrategia y de planificación, de gestión y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización. Los principios que describe está norma corresponden a: crear y proteger el valor, es una parte integral de todos los procesos de la organización, es parte de la toma de decisiones, trata explícitamente la incertidumbre, es sistémica, estructurada y oportuna, se basa en la mejor información disponible, es adaptable, integra los factores humanos y culturales, es transparente y participativa, es dinámica, iterativa, responde a los cambios y facilita la mejora continua de la organización.

Para ejemplificar y basados en la norma 31000 utilizando la metodología para la gestión del riesgo denominada Magerit versión 3 se respondería a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”; es decir, Magerit versión 3 implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que las organizaciones tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Figura 1. Elementos del análisis de riesgos potenciales.

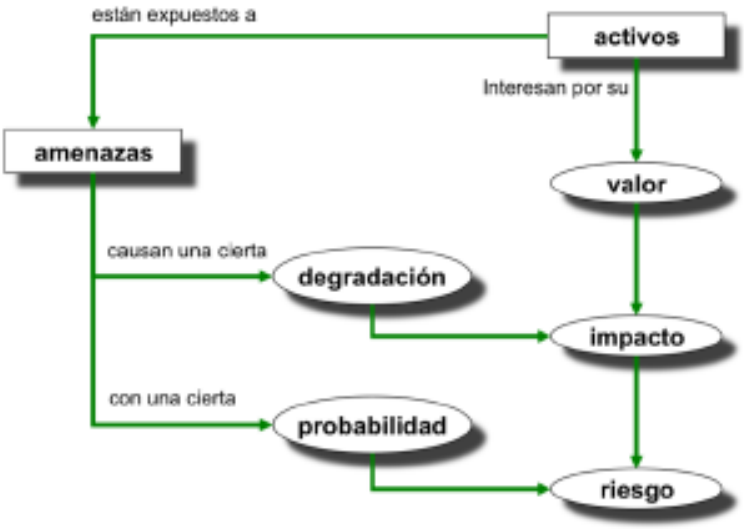


Ilustración 7. Elementos del análisis de riesgos potenciales

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método, 2012. 127 p.

Es así, como la gestión del riesgo pasa a ser una parte fundamental en la administración de la seguridad de la información, permitiendo algunos beneficios, tal como, identificar los puntos más débiles de la estructura de las tecnologías de la Información (TI) que da soporte a los procesos críticos de la organización. Igualmente, además de ser una guía de selección de medidas de protección de costo adecuado, determina dónde es necesario contar con esquemas de recuperación de desastres y continuidad de negocio y permite realizar políticas de seguridad mejor adaptadas a las necesidades de la organización.

En el ámbito de la seguridad de la información, las metodologías de análisis de riesgos conforman una disciplina que se articula desde los Sistemas de Gestión de Seguridad de la Información (SGSI) en las organizaciones, realizando unos importantes escaneos de vulnerabilidades mediante el uso de una serie de modelos y procesos para, así, proponer una forma más segura de cuidar la información y los recursos de tecnologías de la Información (TI). Algunos de los objetivos de las metodologías de análisis de riesgos corresponden a: planificación de la reducción de riesgos, prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas y ayuda en la toma de las mejores decisiones en materia de seguridad de la información.[39]

5.2.6 Magerit versión 3.

Es la metodología de análisis y gestión de riesgos de los sistemas de información de las organizaciones o entidades públicas y privadas elaborada por el Consejo Superior de Administración Electrónica. La razón de ser de Magerit versión 3 está directamente relacionada con la generalización del uso de las tecnologías de Información (TI), que da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

En la introducción de esta metodología sobresalen dos objetivos principales, uno de los cuales es estudiar los riesgos que soporta un sistema de información y el entorno asociado a este, y otro relacionado con recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir impedir, reducir o controlar los riesgos investigados.

[39]«Vista de Metodologías para el análisis de riesgos en los sgsi | Publicaciones e Investigación», accedido 3 de abril de 2020, https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754.

Los principales elementos para el análisis de riesgos, según Magerit versión 3 son: activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguardas (funciones, servicios y mecanismos). De la misma manera, de acuerdo con Magerit versión 3, el proceso de análisis de riesgos se desarrolla en las siguientes etapas: planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas. Magerit versión 3 detalla la metodología desde tres perspectivas: describe los pasos para realizar un análisis del estado del riesgo y gestionar su mitigación; describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos y uno de sus capítulos aplica la metodología al caso del desarrollo de Sistemas de Información (SI). Adicionalmente, muestra una serie de aspectos prácticos derivados de la experiencia acumulada en el tiempo para el análisis y gestión del riesgo de manera efectiva.

Esta metodología ayuda a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y apoyar en la preparación de la organización para procesos de evaluación, auditoría, certificación o acreditación; así mismo, una de sus mayores ventajas es que las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles. Otro de sus aspectos positivos radica en que sus resultados se expresan en valores económicos lo que, a su vez, también es una desventaja por cuanto el hecho de tener que traducir de forma directa todas las valoraciones en valores económicos, hace que la aplicación de esta metodología sea muy costosa.[40]

Magerit versión 3 persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de gestionarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

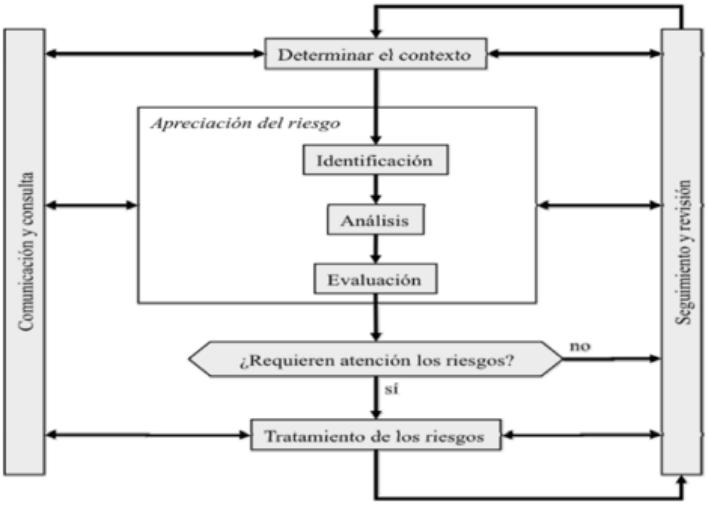
Ventajas de la metodología Magerit versión 3:

- Las decisiones que deban tomarse y que tengan que ser validadas por la dirección estarán fundamentadas y serán fácilmente defendibles.
- Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla.
- Permitirá saber cuánto valor tiene la información o los servicios que maneja la empresa y ayudará a protegerlos.

[40]«Vista de Metodologías para el análisis de riesgos en los sgsi | Publicaciones e Investigación».

- Conocer el riesgo al que están sometidos los elementos de trabajo para poder gestionarlos.
- Tener una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.[41]

Figura 2. Proceso de gestión de riesgos.



Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I – Método, 2012. 127 p.

Actualmente se encuentra vigente MAGERIT versión 3 que integra e implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los interesados tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.[42]

5.3 MARCO EMPRESARIAL

5.3.1 Reseña Histórica

[41]Enrique Ferruzola Gómez et al., «Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT», *Revista Científica y Tecnológica UPSE* 6, n.º 1 (21 de junio de 2019): 34-41, https://doi.org/10.26423/rctu.v6i1.429.

[42]Fabio Adalberto Arellano Montenegro, «REALIZAR EL ANÁLISIS PARA GESTIÓN DE RIESGOS EN LOS SISTEMAS DE INFORMACIÓN DE LA IPS SOLIDARIOS SALUD DEL MUNICIPIO DE CUASPUD CARLOSAMA A PARTIR DE LA NORMA ISO 27001 APLICANDO LA METODOLOGÍA MAGERIT», 2018, 176.

El Laboratorio Clínico Patológico López Correa S.A., es una organización fundada en el año 1.984; creada por dos emprendedores profesionales de la salud, un médico especialista en Patología y Laboratorio Clínico y una Bacterióloga, alianza con la cual quisieron unir sus esfuerzos, y contribuir no solo al desarrollo de su vida personal y profesional, sino también prestar una labor social y de ayuda a la comunidad pereirana.

En sus inicios fue un Laboratorio pequeño, sin demanda y poco especializado, se inició con 2 bacteriólogas, un médico patólogo, una auxiliar de laboratorio clínico, y un histotecnólogo; con el transcurrir del tiempo, el trabajo realizado, el esfuerzo, la dedicación y la gran aceptación por parte del gremio médico y de las diferentes entidades de salud, por su eficiencia y confiabilidad demostrada en los resultados de las pruebas y así mismo con su amplio portafolio de servicios, se fue posicionando en la ciudad y poco a poco en el Eje Cafetero.

A medida que se incrementaron los usuarios se pensó en mejorar tecnológicamente y en brindar alternativas de exámenes que complementaran el diagnóstico médico. En febrero de 2.004 fue la primera institución de salud de Risaralda, en obtener la Certificación de Gestión De Calidad por parte de ICONTEC, la cual ha sido revisada anualmente y recertificada.
Actualmente se tienen todos los procesos sistematizados, desde la atención al cliente, hasta el procesamiento de los exámenes, partiendo de la identificación de muestras por paciente con códigos únicos de barra, los cuales son leídos por los diferentes equipos del Laboratorio a través de interfaces desarrolladas para la trasmisión de la información del software de Laboratorio a los equipos biomédicos.

El Laboratorio tiene implementado un estricto control de calidad, que busca aumentar precisión y exactitud en las pruebas. Se utilizan métodos estadísticos internos y se cuenta con esquemas de evaluación externa de calidad con el Colegio Americano de Patología - CAP - PROASECAL y RIQAS (Entidad avalada internacionalmente por el Standard NTC-ISO 9001), el cual tiene como ventaja comparar el desempeño del Laboratorio López Correa con el de otros laboratorios que utilizan metodologías iguales.
Tiene cuatro sedes de atención ubicadas en sitios estratégicos de la ciudad (Principal, Megacentro Pinares, Cuba, Dosquebradas y Alamos), con una planta física de aproximadamente 2.500 Mts2, se cuenta con 100 personas como parte del recurso humano entre médicos especialistas en patología, enfermera especialista salud ocupacional, bacteriólogos, citohistotecnólogos, auxiliares de laboratorio, auxiliares de enfermería y personal administrativo y de apoyo al cliente.

Siempre el cliente ha sido el eje central de la gestión organizacional, caracterizándose la empresa por la calidez humana al usuario y por el interés en brindar una satisfacción total a sus necesidades y expectativas. El Laboratorio Clínico Patológico López Correa, ofrece confiabilidad, oportunidad y rapidez en la entrega de los resultados, además de una esmerada atención al paciente que muchas veces llega de otras ciudades y/o municipios cercanos a Pereira.
Dentro de las prioridades del Laboratorio siempre ha estado su responsabilidad social, es por eso que ha venido apoyando a través de donaciones de exámenes de laboratorio y de patología, y a través de ayudas económicas y en especie a varias fundaciones, colaborando de esta manera a mejorar la calidad de vida de la comunidad.
La Institución es Laboratorio de referencia y contra referencia a nivel regional, estando catalogados como líderes en tecnología, cobertura y atención, prestando atención a aproximadamente a 145.307 usuarios en el año 2019.

SERVICIOS ESPECÍFICOS QUE SE PRESTAN.
En el cumplimiento de su actividad misional, el Laboratorio presta habitualmente los siguientes servicios:

- Química clínica
- Hematología
- Coagulación
- Inmunología
- Alérgenos
- Microbiología
- Parasitología
- Uroanálisis
- Estudios hormonales con o sin estímulo
- Pruebas de fertilidad
- Marcadores tumorales
- Monitoreo de drogas terapéuticas y de abuso
- Diagnóstico de enfermedades infecciosas y metabólicas
- Test de sudor por iontoforesis para detección de la fibrosis quística del páncreas
- Biología Molecular
- Genética
- Apoyo a Centros de Investigación en estudios clínicos (Certificación IATA)
- Análisis de biopsias simples y múltiples y especímenes quirúrgicos de órganos por condición tumoral benigna o maligna y por condición no tumoral
- Estudios de inmunohistoquímica
- Coloraciones especiales (Bk, hongos)
- Receptores hormonales
- Citología vaginal

- Citología de líquidos, esputo y lavado o cepillado bronquial
- Citología por aspiración con aguja fina
- Prueba para la detección del HPV-Virus del papiloma humano
- Exámenes de ingreso y egreso laboral
- Exámenes médicos con énfasis ergonómico y osteomuscular
- Certificado para trabajo en alturas y espacios confinados
- Exámenes periódicos de salud ocupacional
- Valoración de manipuladores de alimentos
- Exámenes preventivos de riesgo cardiovascular y control laboral
- Chequeos médicos ejecutivos
- Toma de muestras y embalajes

5.3.2 Valores.

Se identifican las siguientes conductas consideradas deseables para orientar el comportamiento interpersonal, tanto a nivel interno como externo:

Amabilidad: Actitud positiva hacia las demás personas. Empatía.
Integridad: Coherencia entre lo que se dice y hace, demostrar en todo sentido honestidad y rectitud.
Respeto: Reconocimiento y consideración en la interacción interpersonal, basados en los derechos individuales.
Responsabilidad: Asumir y cumplir con agrado las tareas encomendadas.
Vocación de servicio: Toma de conciencia sobre las necesidades de los demás, deseo de contribuir y colaborar para superarlas.

5.3.3 Principios.

Se identifican las siguientes conductas deseables en los colaboradores para orientar su comportamiento en lo relacionado con la actividad organizacional:

Adaptabilidad al cambio: Capacidad para adaptarse a los cambios, políticas y adherirse a los procedimientos establecidos.
Aprovechamiento de recursos: Disposición para usar y aprovechar adecuadamente los recursos materiales, bienes y servicios del Laboratorio.
Calidad en el trabajo: Desarrollar acciones prácticas y operables que conduzcan a los resultados esperados por la Organización.
Compromiso: Sentir como propios los objetivos de la Organización, cumpliendo con las responsabilidades asignadas y administrando eficientemente los recursos existentes.
Comunicación efectiva: Capacidad de interactuar activamente con las demás personas, haciendo uso de la empatía, la diplomacia, el asertividad, la escucha

activa y las preguntas adecuadas para garantizar la comprensión del mensaje trasmitido y recibido.
Confidencialidad: Tener prudencia y conservar el secreto profesional, para generar confianza a todas las partes interesadas.
Servicio humanizado: Capacidad de brindar al usuario, una atención cálida, amable, afectuosa, oportuna y flexible, sintiendo su necesidad como propia.
Trabajo en equipo: Habilidad y compromiso para trabajar con los demás, donde cada uno aporta en pro de los objetivos comunes, cuidando los procesos, procedimientos, relaciones interpersonales y la comunicación, para lograr los resultados esperados en un buen ambiente de cooperación.
Veracidad: Brindar verdad, certeza y confiabilidad en los resultados y servicios prestados.

5.3.4 Misión.

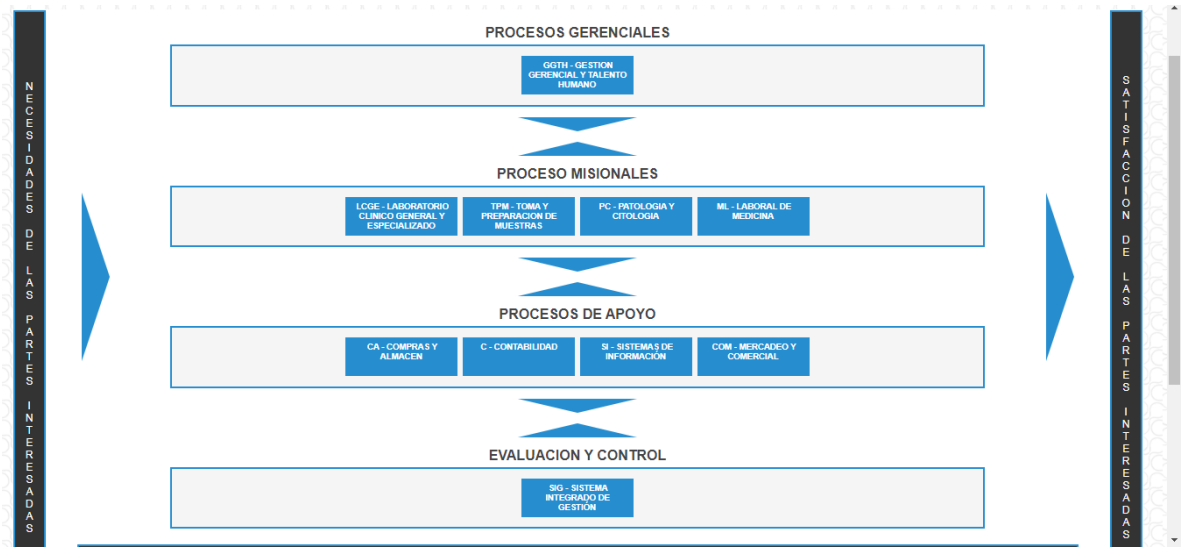
Somos una organización que contribuye efectivamente a la salud de la comunidad en general mediante la prestación de servicios especializados en laboratorio clínico, patología, citología y medicina ocupacional. De igual manera, apoyamos el desarrollo de estudios clínicos de Centros de Investigación nacionales e internacionales.
Estamos comprometidos con la satisfacción de nuestros clientes, colaboradores y demás grupos de interés, brindando una atención oportuna, segura y con calidad humana.
Para lo anterior disponemos de personal calificado, tecnología de última generación y altos estándares de calidad que aseguran la confiabilidad en los resultados.

5.3.5 Visión.

En el año 2022 tendremos presencia y estaremos posicionados en la región del Eje Cafetero y Norte del Valle, como una entidad líder en el sector de la salud, manteniendo la confiabilidad de los resultados, el cumplimiento de los estándares establecidos de calidad y la efectividad en nuestros procesos.

5.3.6 Mapa de Procesos.

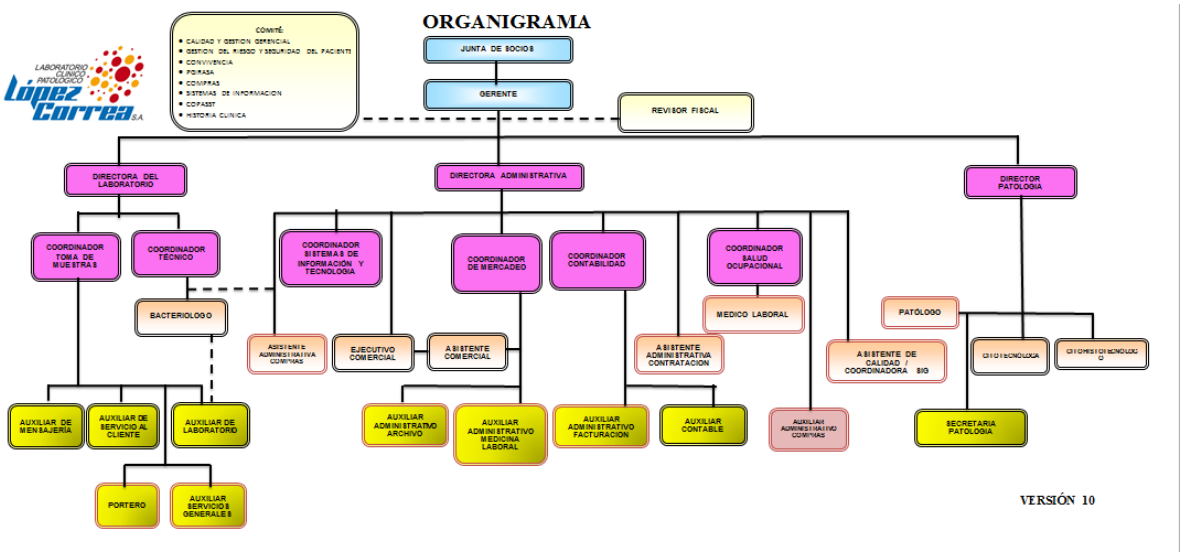
Figura 3. Mapa de procesos.



Fuente: Elaboración Propia

5.3.7 Organigrama.

Figura 4. Organigrama Laboratorio Clínico Patológico López Correa S.A.



Fuente: Manual de Calidad Laboratorio Clínico Patológico López Correa. 2020

5.3.8 Sede Principal.

Centro
Calle 24 N. 5 – 41
Pbx: (6) 3351223
Fax: (6) 3332234
Celulares: 312-2860809 - 315-8146359
Horario de atención:
Lunes a Viernes: 6:30 am – 6:30 pm
Sábados: 7:00 am –12:00 m

Figura 5. Foto Sede Principal – Centro.

Fuente: https://www.lopezcorrea.com/2017/index.php?option=com_content&view=article&id=687&Itemid=1097

5.4 GLOSARIO DE TERMINOS

ACTIVO: Todos los recursos documentales, humanos, tecnológicos y físicos fundamentales para el correcto funcionamiento de la organización tales como hardware, software, manuales, procedimientos, normas, personal, redes, instalaciones, servicios e Información.

ALCANCE: Describe la extensión y los límites del SGSI**,** por lo que puede estar definido en términos de los activos de información, la ubicación física, las unidades organizacionales, actividades o procesos de mayor importancia para la organización, es decir, se trata de la selección de los elementos críticos a proteger**.**

ANALISIS DE RIESGOS: Es el proceso que comprende la naturaleza del riesgo y determina su nivel de gravedad.

AMENAZA: Suceso o situación que se presenta en las organizaciones que desencadenan en incidentes causando efectos negativos ocasionando daños materiales o perdidas de los activos de información.

ATAQUE: Intentar destruir, exponer, alterar, deshabilitar, robar o tener acceso no autorizado de un activo. Un ciberataque es aquel acto mal intencionado contra un sistema informático, una red o una aplicación.

COMPETITIVIDAD: Característica que debe tener una organización para perdurar en el mercado, es la capacidad de mantener de una forma sistémica ventajas comparativas para alcanzar, sostener y mejorar su posición en el entorno.

CONFIDENCIALIDAD: Garantía de reserva del acceso a la información únicamente a personas autorizadas con el fin de salvaguardar los datos de intrusos no deseados. Esta propiedad es uno de los pilares de los sistemas de seguridad de la información.

CONFORMIDAD: Es el cumplimiento de los requisitos del sistema de seguridad de la información bajo la Norma NTC/ISO/IEC 27001:2013.

CONTROL: Medida de protección que se establece dentro de la organización para evitar, mitigar o eliminar los riesgos salvaguardando la información por medio de políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

DIAGNOSTICO: Es el proceso sistemático de reconocimiento, análisis y evaluación de una situación para determinar sus tendencias o darle solución a un problema a partir de observaciones y datos reales.

DISPONIBILIDAD: Es la capacidad que tiene una persona autorizada de acceder a la información requerida y en un formato correcto cuando lo desee o bien considere necesario. Esta propiedad es uno de los pilares de los sistemas de seguridad de la información.

DOCUMENTAR: Acción de evidenciar por medio de un conjunto de documentos y registros una información específica en su medio de soporte.

EFECTIVIDAD: Grado en que se logra el cumplimiento de las actividades planificadas en los objetivos de la seguridad de la información.

GESTIÓN DE RIESGO: Es el proceso sistemático de identificar, analizar, tratar y controlar los riesgos asociados a la seguridad de la información a que está expuesta la organización.

GESTIÓN DE INCIDENTES: Es el proceso para detectar, reportar, evaluar, responder y tratar los incidentes de la seguridad de la información.

INCIDENTE: Evento inesperado o no deseado que tiene una probabilidad significativa de materializarse comprometiendo las operaciones organizacionales y amenazando la seguridad de la información. Estos sucesos tienen que ser atendidos por una estructura de gestión de incidencias.

INDICADOR: Medida que proporciona una estimación o evaluación para la toma de decisiones. Para la seguridad de la información sirven como evidencia de posibles delitos en un sistema o una red el cual permiten analizar y mejorar las técnicas y comportamientos ante una amenaza en particular.

INFORMACIÓN: Es el conjunto de datos organizados y procesados para su comprensión contenidos en algún documento que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad informática. La información es el activo más importante de la organización y por lo tanto necesita ser protegido.

INTEGRIDAD: Es la preservación de la información completa y exacta. Se refiere a como los datos se mantienen intactos, libres de modificaciones o alteraciones accidentales o mal intencionadas. Esta propiedad es uno de los pilares de los sistemas de seguridad de la información.

ISO: Es la Organización Internacional de Normalización con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

METODOS: Es un modo, manera o forma de realizar algo de forma sistemática, organizada y/o estructurada.

MITIGAR: El propósito de la mitigación es la reducción de la vulnerabilidad.

PHVA (Planear – Hacer – Verificar – Actuar): Es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo es muy utilizado para implantación de sistemas de gestión, como los sistemas de gestión de la calidad que muchas empresas de hoy lo implantan para la calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua.

POLITICA DE SEGURIDAD: Un conjunto de directrices, normas, procedimientos, que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados en la Empresa, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico.

PROCESOS: Conjunto de actividades relacionadas entre sí, transformando elementos de entrada en elementos de salida.

PROTECCIÓN: Capacidades de defensa frente a amenazas.

RECURSOS: Elementos que pueden utilizarse como medios a efectos de alcanzar un propósito determinado.

REQUISITOS: Necesidad o expectativa que pueden ser expresadas, normalmente implícitas o impuestas. Pueden existir requisitos del cliente, requerimientos de la norma, requisitos internos de la organización, requisitos reglamentarios y legales, entre otros.

RIESGO: Contingencia o proximidad de un daño.

SALVAGUARDAR: Corresponde al hecho de que se tengan los datos sin posibilidad de perderlos, siempre a salvo y con posibilidad de recuperarlos en caso de cualquier tipo de incidente.

SEGURIDAD DE LA INFORMACIÓN: Son aquellas medidas preventivas y reactivas de una Organización que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma.

SEGURIDAD INFORMATICA: Es la que permite lograr que todos los sistemas informáticos utilizados en cualquier contexto se encuentren seguro de cualquier daño o riesgos, ya sea por parte de personas ajenas que en forma voluntaria o involuntaria lo pueda hacer o de cualquier desastre natural. En este sentido, la protección de la información requiere de un conjunto de software o aplicativos diseñados, documentos estándares y metodologías existentes que permitan aplicar las normativas certificables internacionalmente y técnicas apropiadas para llevar un control en la seguridad.

TECNOLOGIA: Conjunto de instrumentos, métodos y técnicas diseñados para resolver un problema. Es el estudio, la investigación, el desarrollo y la innovación de las técnicas y procedimientos, aparatos y herramientas que son empleados para la transformación de materias primas en objetos o bienes de utilidad práctica.

TIC: Tecnologías de la Información y la Comunicación**,** este concepto hace referencia a las teorías, las herramientas y las técnicas utilizadas en el tratamiento y la transmisión de la información: informática, internet y telecomunicaciones.

VULNERABILIDAD: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

5.5 MARCO NORMATIVO

Tabla 1. Marco normativo.

NORMA	AÑO	DESCRIPCION
Ley 1266	2008	Habeas Data. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras

NORMA	AÑO	DESCRIPCION
		disposiciones. Esta ley desarrolla una regulación integral del derecho fundamental de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos y en archivos de entidades públicas y privadas
Resolución 4505	2012	Por la cual se establece el reporte relacionado con el registro de las actividades de Protección Específica, detección Temprana y la aplicación de las Guías de Atención Integral para las enfermedades de interés en salud pública de obligatorio cumplimiento
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Norma Técnica Colombiana NTC/ISO/IEC 27001:2013	2013	Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.
Decreto Único 1074	2015	Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, relacionado con el plazo para llevar a cabo el registro de las bases de datos
Guia Técnica Colombiana GTC - ISO/IEC 27002:2015	2015	Tecnologías de la Información. Técnicas de seguridad. Código de practica para controles de seguridad de la información.
Resolución 256	2016	Por la cual se dictan disposiciones en relación con el Sistema de Información para la Calidad y se establecen los indicadores para el monitoreo de la calidad en salud
Circular Externa No. 001 Superintendencia de Industria y Comercio	2016	Impartir instrucciones a los a los responsables del Tratamiento de datos personales, personas naturales, entidades de naturaleza pública distintas de las sociedades de economía mixta y personas jurídicas de naturaleza privada que no están inscritas en las cámaras de comercio, para efectos de realizar la inscripción de sus bases de datos

NORMA	AÑO	DESCRIPCION
		en el Registro Nacional de Bases de Datos – RNBD
Circular externa 02 de Supersalud	2020	Por la cual impartió instrucciones a las entidades sometidas a su inspección, vigilancia y control, en relación con la transmisión y retransmisión de información a través de los sistemas de recepción, validación y cargue

Fuente: Elaboración Propia

6 HIPÓTESIS Y VARIABLES

Esta investigación no contempla hipótesis por ser un estudio descriptivo documental.

Variables:

Tabla 2. Variables.

OBJETIVOS ESPECÍFICOS	CONCEPTOS	DEFINICIÓN	VARIABLES	DEFINICIÓN	CATEGORÍAS	DEFINICIÓN	INDICADORES
Diagnosticar el servicio de información actual de la empresa frente a los requisitos de la norma	Diagnostico	Es el proceso de reconocimiento, análisis y evaluación de una cosa o situación para determinar sus tendencias o solucionar un problema	Reconocimiento	Examinar un objeto o una persona para percibir su naturaleza y su identidad o circunstancias	Situación reconocida	Identificación de situación observada	Número de situaciones diagnosticadas
	Laboratorio Clínico Patológico López Correa	Sede principal Laboratorio Clínico Patológico López Correa					Un (1) Laboratorio Clínico Patológico López Correa
Identificar las diferencias entre el servicio actual y los requisitos de la norma.	Sistemas de información	Conjunto de elementos que interactúan entre sí con un fin común; que permite que la información esté disponible para satisfacer las necesidades en una organización.	Disponibilidad	Todo aquello que se puede utilizar libremente	Disponible	Accesible al uso	Cantidad de Información disponible
					No disponible	No accesible al uso	
	ISO 27001:2013	Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.	Seguridad de la información	Preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización	Requisitos exigibles	Necesidad o expectativa establecida generalmente implícita u obligatoria	% de cumplimiento de los requisitos = (Requisitos cumplidos/ Requisitos totales exigibles) x 100
Definir la metodología de gestión del riesgo e implementarla en el sistema de gestión de seguridad de la información de la empresa.	Gestión del Riesgo	Es el proceso sistemático de identificar, analizar, tratar y controlar los riesgos asociados a la seguridad de la información a que está expuesta la organización.	Riesgos	Contingencia o proximidad de un daño	Mitigación	Acciones para reducir la vulnerabilidad a ciertos peligros	% Cumplimiento de la metodologia de gestión de riesgos
					Aceptación	Admisión y tolerarancia de un riesgo por considerarlo bajo y con pocas probabilidades de ocurrencia	
Elaborar la documentación requerida en la fase de planeación del Sistema de Gestión de la Seguridad de la Información bajo los requisitos de la norma	Documentación	Es la ciencia que consiste en documentar, ésta se encuentra identificada por el procesamiento de información que otorgará datos específicos sobre un tema determinado	Documentar	Soporte o medio que contiene información de interés para la organización	Sistema de gestión de la seguridad de la información	Conjunto de elementos que interactúan entre sí en una organización para el establecimiento de Políticas, objetivos y Procesos, con la meta de alcanzar dichos objetivos.	Cantidad de Información documentada

Fuente: Elaboración Propia.

7 MÉTODO O ESTRUCTURA DE LA UNIDAD DE ANÁLISIS, CRITERIOS DE VALIDEZ Y CONFIABILIDAD

7.1 UNIDAD DE ANÁLISIS

Numerales de la Norma NTC/ISO/IEC 27001:2013.

7.2 CRITERIOS DE VALIDEZ

Lista de chequeo de la Norma NTC/ISO/IEC 27001:2013.

7.3 CONFIABILIDAD

Se obtiene con el uso del instrumento (Norma NTC/ISO/IEC 27001:2013) de ser obtenido de una norma internacional emitida por la organización internacional de normalización.

8 DISEÑO METODOLÓGICO

Trabajo de investigación, descriptiva documental aplicada.

8.1 FUENTES DE INFORMACIÓN

Primarias: Norma NTC/ISO/IEC 27001:2013, GTC-ISO/IECN27002:2015, Procesos y procedimientos, Correos electrónicos, listas de chequeo y conocimientos previos.

Secundarias: Bases de datos, Software Cóndor Suite, Manual de Calidad, documentos y registros

8.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Lista de chequeo obtenida de la NTC/ISO/IEC 27001:2013 y el Anexo A.

8.3 POBLACIÓN Y MUESTRA

Para esta población y muestra estarán constituidos por la Norma NTC/ISO/IEC 27001:2013 con todos los numerales y el Anexo A.

9 ESQUEMA TEMÁTICO

Tabla 3. Esquema temático.

TEMAS	SUBTEMAS
Problema	Planteamiento Formulación Sistematización
Justificación	Metodológica Teórica Práctica
Objetivos	General Específicos
Marco referencial	Marco antecedentes Marco conceptual Marco empresarial Glosario de términos Marco normativo
Diseño metodológico Lógico	Fuentes de información Técnicas de recolección de información Población y muestra
Resultados	Análisis Discusión
Conclusiones	
Recomendaciones	

Fuente: Elaboración Propia

10 PERSONAS QUE PARTICIPAN

Tabla 4. Personas que participan.

DIRECTOR DE LA INVESTIGACIÓN	Fernando Jaime Escobar – Ingeniero en Sistemas

INVESTIGADORAS	Laura Lorena Tobón Quiceno - Ingeniera Industrial Alexandra Alarcón Posso- Administradora Industrial

Fuente: Elaboración Propia

11 RECURSOS DISPONIBLES

Tabla 5. Recursos disponibles.

PRESUPUESTO	$ 5.700.000
RECURSOS HUMANOS	$1.200.000 20 horas Director del proyecto
	$3.600.000 120 horas por Investigadoras
RECURSOS LOGÍSTICO (Transporte y alimentación)	$300.000
RECURSOS TECNOLOGICOS (Internet, energía, hora computador)	$600.000

Fuente: Elaboración Propia

12 CRONOGRAMA

Tabla 6. Cronograma.

OBJETIVOS	ACTIVIDAD	MESES						
		Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Diagnosticar el servicio de información actual de la empresa frente a los requisitos de la norma.	Diseñar herramienta para desarrollar el análisis del servicio de información.	X						
	Realizar análisis del servicio de información del laboratorio.	X						
	Consolidar resultados y realizar diagnostico actual del servicio de información del laboratorio	X						
Identificar las diferencias entre el	Comparar el diagnostico actual del servicio de información del laboratorio frente a los requisitos de la norma.	X						

servicio actual y los requisitos de la norma.	Identificar diferencias y faltantes del servicio de información del laboratorio.		X					
	Realizar análisis por cada numeral de la norma de acuerdo con las diferencias y faltantes encontradas en el servicio de información del laboratorio.		X					
Definir la metodología de gestión del riesgo e implementarla en el sistema de gestión de seguridad de la información de la empresa.	Identificar la metodología de gestión del riesgo adecuada para el laboratorio mediante un análisis comparativo de ventajas y desventajas entre cinco metodologías seleccionadas.		X					
	Realizar lectura de los 3 libros de la metodología elegida de Magerit 3.0.		X					
	Implementar metodología Magerit 3.0 en el sistema de la información del laboratorio.			X				
	Realizar matriz y tratamiento de del riesgo del laboratorio			X	X			
	Elaborar guía de implementación de la matriz de riesgo del laboratorio según la metodología Magerit 3.0.			X	X			
	Realizar recomendaciones generales de acuerdo con el análisis de riesgos.				X	X		
Elaborar la documentación requerida en la fase de planeación del Sistema de Gestión de la Seguridad de la Información bajo los requisitos de la norma.	Definir la fase de PHVA en la matriz de controles basados en el anexo A de la norma NTC/ISO/IEC 27001:2013					X		
	Filtrar los controles de la fase de Planear y realizar un análisis de cumplimiento.					X	X	
	Realizar recomendaciones para darle cumplimiento a los controles identificados de la fase de Planear.					X	X	
	Identificar la documentación necesaria en la fase de planeación para darle cumplimiento a los requisitos de la norma.						X	X
	Elaborar la documentación requerida en la fase de planeación según la norma						X	X

	Presentar a la Dirección la fase de planeación del Sistema de Seguridad de la Información del laboratorio							X

Fuente: Elaboración Propia

13 COMPONENTES DE LA INVESTIGACIÓN

13.1 COMPONENTE ÉTICO

Para la investigación se tendrán en cuenta las normas éticas colombianas para realización de trabajos de grado, se contará con el consentimiento institucional descrito en el Anexo 1 – Carta de consentimiento laboral.

13.2 COMPONENTE MEDIOAMBIENTAL

Los investigadores se responsabilizan de minimizar los daños al medio ambiente manejando la información en medio magnética.

13.3 RESPONSABILIDAD SOCIAL

Beneficios obtenidos:

- La Gerencia recibirá apoyo para la seguridad de la información.
- Ayudará a identificar los activos de información y a protegerlos adecuadamente.
- Incrementará sustancialmente los controles de acceso a la información.
- Minimizará la interrupción en el funcionamiento de las actividades del negocio y lo protege de desastres y fallas mayores.
- Generará confianza a los clientes y los socios estratégicos por la garantía de calidad y confidencialidad de los datos.

14 DESARROLLO DEL PROYECTO

14.1 DIAGNOSTICAR EL SERVICIO DE INFORMACIÓN ACTUAL DE LA EMPRESA FRENTE A LOS REQUISITOS DE LA NORMA.

El diagnóstico del servicio actual del Laboratorio Clínico Patológico López Correa frente a los requisitos de la norma NTC/ISO/IEC 27001:2013 y el anexo A, se realizó por medio de la elaboración y diligenciamiento de una herramienta diagnóstico que arrojó los siguientes resultados:

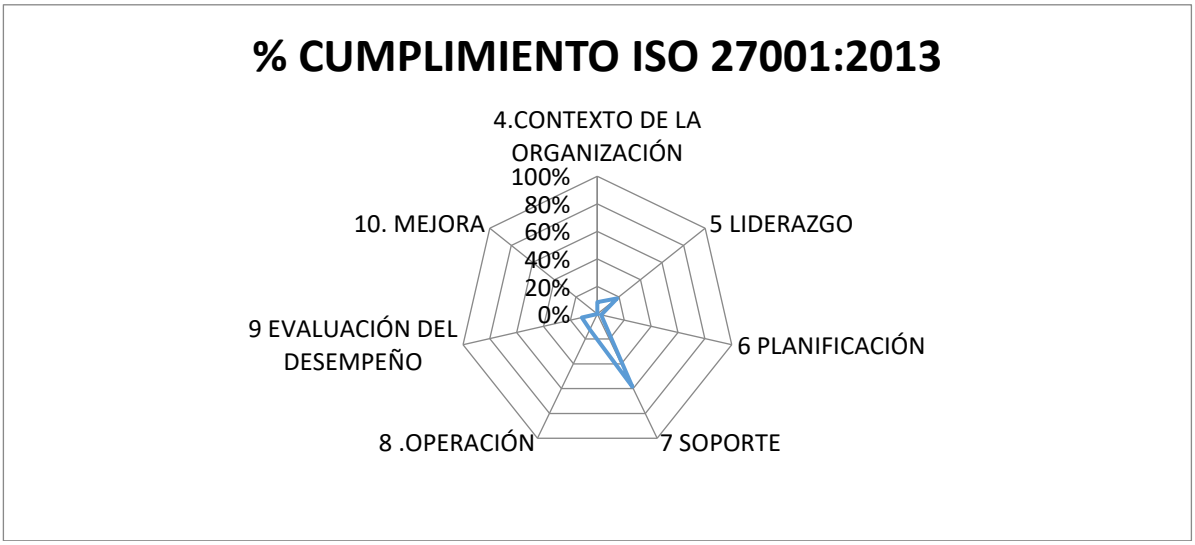
En los resultados obtenidos de la aplicación de la herramienta diagnóstico frente a los numerales de la norma NTC/ISO/IEC 27001:2013 se calculó el porcentaje total de cumplimiento de adecuación siendo del **16%**. En donde el numeral 7 Soporte alcanzó el mayor porcentaje de 58% mientras que los numerales 6 Planificación y 10 Mejora alcanzaron un porcentaje 3% y 0% respectivamente catalogándose como los numerales de menor cumplimiento y los cuales requerirán una mayor atención, como se describe en la siguiente tabla: Anexo 2 – Lista de chequeo ISO 27001.

Tabla 7. Lista de chequeo numerales.

CUMPLIMIENTO REQUISITOS ISO 27001:2013	
NUMERALES	**%**
4.CONTEXTO DE LA ORGANIZACIÓN	9%
5 LIDERAZGO	18%
6 PLANIFICACIÓN	3%
7 SOPORTE	58%
8. OPERACIÓN	13%
9 EVALUACIÓN DEL DESEMPEÑO	12%
10. MEJORA	0%
% CUMPLIMIENTO ADECUACION	**16%**

Fuente: Elaboración propia.

Gráfico 1. Porcentaje de cumplimiento numerales.



Fuente: Elaboración propia.

En los resultados obtenidos de la aplicación de la herramienta diagnóstico frente al anexo A de la norma NTC/ISO/IEC 27001:2013 se calculó el porcentaje total de cumplimiento de adecuación siendo del **22%**. En donde el control A7 Seguridad de los Recursos Humanos y el control A17 Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio alcanzaron el mayor porcentaje de 67% y 63% respectivamente mientras que los controles A9 Control de Acceso, A10 Criptografía, A15 Relaciones con los Proveedores y A18 Cumplimiento, alcanzaron un porcentaje del 0% catalogándose como los anexos sin ningún tipo de control y los cuales requerirán una mayor atención, como se describe en la siguiente tabla: Anexo 3 - Lista de chequeo controles anexo A 27001.

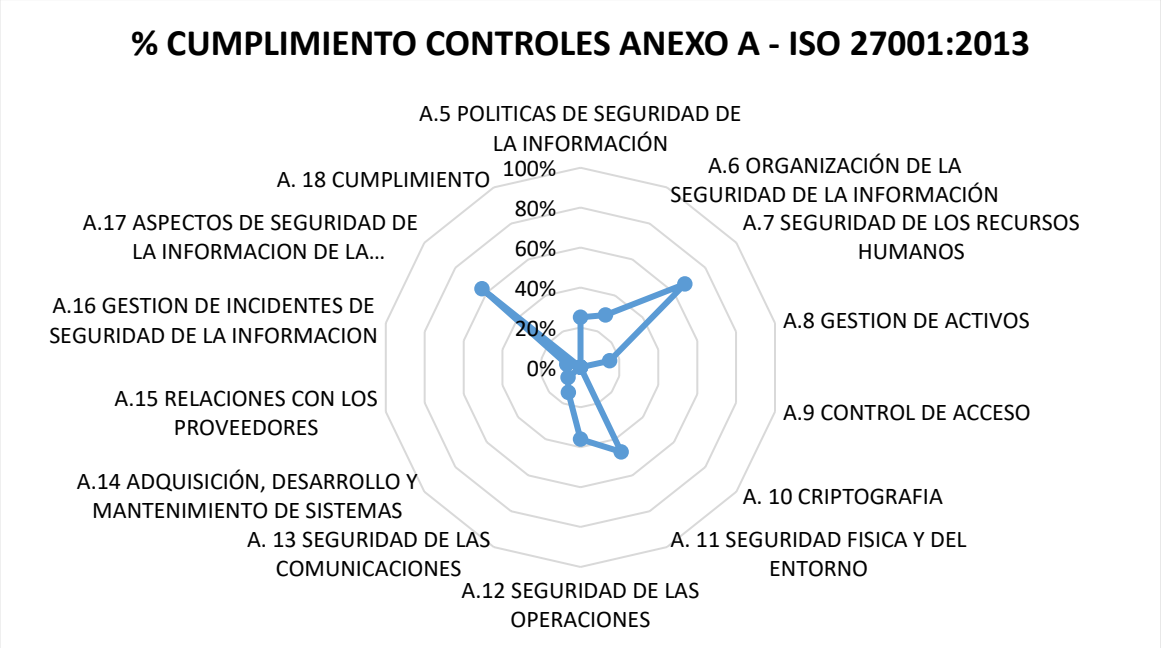
Tabla 8. Lista de chequeo controles.

CUMPLIMIENTO CONTROLES ISO 27001:2013	
ANEXO A	**%**
A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	25%
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	29%
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	67%
A.8 GESTION DE ACTIVOS	15%
A.9 CONTROL DE ACCESO	0%
A. 10 CRIPTOGRAFIA	0%
A. 11 SEGURIDAD FISICA Y DEL ENTORNO	47%
A.12 SEGURIDAD DE LAS OPERACIONES	36%
A. 13 SEGURIDAD DE LAS COMUNICACIONES	14%

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	8%
A.15 RELACIONES CON LOS PROVEEDORES	0%
A.16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	7%
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	63%
A. 18 CUMPLIMIENTO	0%
% CUMPLIMIENTO ADECUACION	**22%**

Fuente: Elaboración propia.

Gráfico 2. Porcentaje de cumplimiento controles.



Fuente: Elaboración propia.

14.2 IDENTIFICAR LAS DIFERENCIAS ENTRE EL SERVICIO ACTUAL Y LOS REQUISITOS DE LA NORMA.

- Se identificaron las siguientes diferencias del servicio actual del Laboratorio Clínico Patológico López Correa frente a los requisitos de la norma NTC/ISO/IEC 27001:2013:

En el numeral 4 **CONTEXTO DE LA ORGANIZACIÓN** con un porcentaje de cumplimiento del 9% se identificó que se debe incluir el análisis del SGSI en el

contexto de la organización, adicional estructurar mejor este proceso incluyendo las partes interesadas, se debe definir el alcance y extender su cumplimiento a todos los procesos.

En el numeral 5 **LIDERAZGO** con un porcentaje de cumplimiento del 18% se identificó que si bien existe compromiso de la dirección para la disponibilidad de recursos para el SGSI la toma de estas decisiones es tardía. Existe un interés en el proceso, pero no hay seguimiento a la implementación de los requisitos y no está claramente definido el aseguramiento de los resultados previstos. Para el seguimiento a las actividades del SGSI existe un comité de seguridad de la información. Es necesario concientizar e involucrar a todo el personal sobre el papel que desarrolla dentro de la seguridad de la información de la empresa. Para las mejoras que se realizan en el proceso se debe lograr que sean preventivas y no correctivas, y lograr la interoperabilidad entre áreas, definiendo roles y mejorando los canales de comunicación.

No existe en la organización la política de la seguridad de la información que sea compatible con la dirección estratégica de la organización y no está establecida como información documentada. No se encuentran formalizados los roles, responsabilidades y autoridades en el proceso de Seguridad de la Información, sin embargo, existe un comité y personas involucradas en el mismo.

En el numeral 6 **PLANIFICACIÓN** con un porcentaje de cumplimiento del 3% se identificó que en la organización no hay planeación de un sistema de gestión de riesgos, no están definidos los riesgos y las oportunidades del SGSI, por lo tanto, no existe el proceso de valoración y tratamiento de riesgos de la seguridad de la información, Los objetivos de la seguridad de la información son medibles y se conservan como información documentada sin embargo no son comunicados ni actualizados periódicamente y no se tiene una adecuada planificación de ellos.

En el numeral 7 **SOPORTE** con un porcentaje de cumplimiento del 58% se identificó que la organización determina y proporciona los recursos necesarios para el total desarrollo del SGSI, también determina y asegura la competencia necesaria de las personas que intervienen en el desempeño de la seguridad de la información y evalúa la eficacia de las acciones tomadas, conservándose de todo ello información documentada. Sin embargo, no existe toma de conciencia en la organización ni está determinada la comunicación interna y externa pertinentes al SGSI.

El laboratorio al tener documentado el Sistema de Gestión de la Calidad bajo la norma ISO 9001:2015 y al estar bajo una estructura de alto nivel, ya se encuentra

definida y establecida en la información documentada de la empresa muchos requisitos de la norma NTC/ISO/IEC 27001:2013 referentes del anexo A, siendo necesario únicamente incluir, conservar y mantener la información documentada concerniente al SGSI.

En el numeral 8 **OPERACIÓN** con un porcentaje de cumplimiento del 13% se identificó que la organización no planifica, implementa y controla procesos necesarios para cumplir los requisitos de seguridad de la información y el cumplimiento de los objetivos. Los procesos contratados externamente (página web) no están controlados. La organización no lleva a cabo valoraciones de riesgo ni tiene implementado un plan de tratamiento de riesgos de la seguridad de la información.

En el numeral 9 **EVALUACIÓN DEL DESEMPEÑO** con un porcentaje del cumplimiento del 12% se identificó que la organización no conserva información documentada de la evaluación del desempeño de la seguridad de la información, no tiene determinado los métodos y periodicidad de seguimiento, medición, análisis y evaluación. No obstante, existe un responsable de la seguridad de la información quien es el encargado del sistema de información. No se realiza auditoría interna al servicio de información, ya que aún no se encuentra estructurado el SGSI.

Existe un comité de Tecnologías de la Información donde se realiza la revisión por la dirección del seguimiento y evaluación del sistema de información, sin embargo, no se realiza revisión del cumplimiento de los objetivos de la seguridad de la información, no se retroalimenta a las partes interesadas, ni se revisa oportunidades de mejora continua. Tampoco se conserva información documentada como evidencia de los resultados de la revisión por la dirección

En el numeral 10 **MEJORA** con un porcentaje del cumplimiento del 0% se identificó que en la organización no existe un programa de no conformidades y acciones correctivas ni de mejora continua, actuando únicamente hacia la corrección y no a la prevención.

- Se identificaron las siguientes diferencias del servicio actual del Laboratorio Clínico Patológico López Correa frente a los controles del anexo A de la norma ISO NTC/ISO/IEC 27001:2013:

En el anexo A5 **POLITICAS DE SEGURIDAD DE LA INFOMACIÓN** con un porcentaje de cumplimiento del 25% se identificó que en la organización existen directrices orientadas a la seguridad de la información las cuales no están definidas

como políticas ni son sometidas a revisión, por lo tanto, dicho control no está implementado. Por parte de la dirección no se brinda completamente orientación y soporte para la gestión de la seguridad de la información ni con las leyes y reglamentos pertinentes.

En el anexo A6 **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** con un porcentaje de cumplimiento del 29% se identificó qué en el control para iniciar la implementación de un SGSI, se cumple parcialmente los roles y responsabilidades para la seguridad de la información, la separación de deberes, el contacto con grupos de interés especial y en la seguridad de la información en la gestión de proyectos; mientras que no cumple con el contacto con grupos de interés especial. No existe control para garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

En el anexo A7 **SEGURIDAD DE LOS RECURSOS HUMANOS** con un porcentaje de cumplimiento del 67% se identificó que la organización cumple con los controles antes de asumir el empleo en la selección de personal idóneo y en todos los términos y condiciones del empleo, igualmente durante la ejecución de este con los controles de procesos disciplinarios, y parcialmente con la responsabilidad de la dirección y con la toma de conciencia, educación y formación en la seguridad de la información. No existe control en el cambio o terminación del empleo ni información documentada al respecto.

En el anexo A8 **GESTIÓN DE ACTIVOS** con un porcentaje de cumplimiento del 15% se identificó que la organización cumple parcialmente el control sobre la protección de los activos organizacionales en inventario, propiedad y uso aceptable, pero no se cumple con el control en la devolución de los activos por lo tanto se requiere un proceso que proporcione trazabilidad. No existe un nivel apropiado de protección en la clasificación de la información, etiquetado de la información y manejo de activos y no hay un proceso definido del manejo de medios de soporte que asegure la prevención de divulgación, modificación, retiro o destrucción de la información almacenada en estos medios.

En el anexo A9 **CONTROL DE ACCESO** con un porcentaje de cumplimiento del 0% se identificó que en la organización no existe ningún tipo de control que limite el acceso a información y a instalaciones de procesamiento de información, ni de rendición de cuentas por la custodia de la información de autenticación, ni tampoco un control que prevenga el uso no autorizado de sistemas y aplicaciones.

En el anexo A10 **CRIPTOGRAFIA** con un porcentaje de cumplimiento del 0% se identificó que en la organización no existe un control en la gestión de llaves criptográficas ni una política sobre el uso de controles criptográficos.

En el anexo A11 **SEGURIDAD FISICA Y DEL ENTORNO** con un porcentaje de cumplimiento del 47% se identificó que la organización no tiene un adecuado control en mantener las áreas seguras las cuales no están completamente prevenidas del acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización existiendo un control parcial únicamente en la protección contra amenazas externas y ambientales y el trabajo en áreas seguras. A diferencia del control a los equipos en los cuales tienen protección completa en su ubicación, mantenimiento, restauración, disposición y retiro de activos.

En el anexo A12 **SEGURIDAD DE LAS OPERANCIONES** con un porcentaje de cumplimiento del 36% se identificó que en la organización el único control a los procedimientos, operaciones y responsabilidades es un procedimiento documentado. Existe control parcial contra los códigos maliciosos y copias de respaldo, también parar el registro y seguimiento de eventos e igualmente en el control de software operacional. En la gestión de la vulnerabilidad técnica hace falta documentar y los perfiles no se han definido. No existe control de auditorías del sistema de información.

En el anexo A13 **SEGURIDAD DE LAS COMUNICACIONES** con un porcentaje de cumplimiento del 14% se identificó que en la organización no hay control de redes, hay control parcial en la seguridad de los servicios de red y hace falta tener separada la red para los clientes a la red corporativa. No existe ningún control para la transferencia de información (políticas, procedimientos, acuerdos de confidencialidad).

En el anexo A14 **ADQUICISIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** con un porcentaje de cumplimiento del 8% se identificó que la organización no hay cumplimiento en el control para seguridad de servicios de las aplicaciones en redes públicas, sin embargo, tiene un control parcial en el resto de los requisitos de seguridad de los sistemas de información en donde hace falta medir y testear. No existe seguridad en los procesos de desarrollo y de soporte ni en los datos usados para pruebas.

En el anexo A15 **RELACIONES CON LOS PROVEEDORES** con un porcentaje de cumplimiento del 0% se identificó que en la organización no existe ningún tipo de

control para la seguridad de la información en las relaciones con los proveedores (políticas de seguridad, acuerdos, cadena de suministros) ni en la gestión de la presentación de servicios de proveedores (seguimiento y revisión y gestión del cambio).

En el anexo A16 **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** con un porcentaje de cumplimiento del 7% se identificó que en la organización no existe control para la gestión de incidentes y mejoras en la seguridad de la información, no hay auditorias que evalúen los eventos y sean clasificados como incidentes y únicamente se tiene establecidas parcialmente las responsabilidades y los procedimientos de gestión.

En el anexo A17 **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO** con un porcentaje de cumplimiento del 63% se identificó que la organización se asegura completamente de tener disponibilidad de las instalaciones de procesamiento de información. Sin embargo, tiene un cumplimiento parcial sobre la continuidad de la seguridad de la información en su planeación, implementación, verificación, revisión y evaluación.

En el anexo A18 **CUMPLIMIENTO** con un porcentaje de cumplimiento del 0% se identificó que la organización no tiene cumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad, específicamente en la aplicación de la ley 1273 de 2009, por lo tanto, la empresa no asegura que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.

14.3 DEFINIR LA METODOLOGÍA DE GESTIÓN DEL RIESGO E IMPLEMENTARLA EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA.

La metodología de gestión del riesgo que decidimos implementar en el Sistema de Gestión de la Seguridad de la Información del Laboratorio Clínico Patológico López Correa es **MAGERIT 3.0** de acuerdo con el análisis realizado de las ventajas y desventajas de cinco metodologías seleccionadas, descritas en el siguiente comparativo:

Tabla 9. Comparativo metodologías de gestión del riesgo.

METODOLOGIAS	MAGERIT 3.0	OCTAVE	MEHARI	ISO / IEC 27005	CRAMM
VENTAJAS	*No tiene costo y no requiere autorización para su uso ya que es una normativa de libre aplicación. *Alcance completo en el análisis y gestión de riesgos. *Está bien documentada en cuanto a recursos de información, amenazas y tipos de activos. *Plantea un análisis de costo beneficio, expresa una fórmula de ROI (Retorno de la Inversión) *Es metódica por lo que se hace fácil su comprensión. *Los activos se identifican. *Tipifican, se buscan sus dependencias, se valoran en cuanto a: disponibilidad, confidencialidad, autenticidad, integridad y trazabilidad. *Usa un modelo de análisis de riesgos cualitativos y cuantitativos. *Soporta herramientas comerciales y no comerciales, así como las normas ISO/IEC 27001, ISO/IEC 15408 e ISO/IEC 17799.	*Cualquier metodología que aplica los criterios de principio, atributos y resultados es considerado compatible con esta metodología. *Involucra todo el personal. *Es auto dirigible. *Involucra como elementos de su modelo de análisis: procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas. *Uso interno gratuito.	*Tiene la capacidad de evaluar y simular los niveles de riesgos derivados de las medidas adicionales. *Soporta herramientas comerciales y no comerciales. *Es compatible con el estándar ISO/IEC 27001, ISO/IEC 27005. *Usa un modelo de análisis de riesgos cualitativos y cuantitativos. *Es una metodología para la gestión del riesgo.	*Aborda los riesgos de forma oportuna y eficaz. *Ayuda a crear un SGSI. *Permite identificar las necesidades de las organizaciones sobre los requisitos de la seguridad de la información. *Considera análisis cuantitativos y cualitativos.	*Realiza un análisis de riesgos cuantitativos y cualitativos. *Identifica y clasifica los activos de TI. *Evalúa el impacto empresarial. *Combina análisis y evaluación de riesgos. *Es aplicable a todo tipo de sistemas y redes de información. *Compuesta por más de 4000 contramedidas divididas en grupos y subgrupos.
DESVENTAJAS	*No tiene en cuenta el principio de no repudio de la información. *La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión y evaluación. *La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos. *No toma en cuenta un análisis de vulnerabilidades.	*Para el uso externo se debe comprar una licencia al SEI si se quiere implementar una metodología a un tercero. *Es una metodología aplicable solo para Pyme, mediana o pequeña empresa. *No tiene en cuenta el principio de repudio de la información. *Utiliza muchos documentos en el proceso de análisis de riesgos. *No tiene compatibilidad con estándares.	*No tiene en cuenta el principio de no repudio de la información. *La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión. *La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.	*No recomienda una metodología específica para la gestión de riesgos en la seguridad de la información.	*La versión 4 tiene costo de mantenimiento anual. *En su modelo no tiene contemplados elementos como los procesos y los recursos.

Fuente: Elaboración propia.

Cabe aclarar que la metodología Magerit 3.0 será aplicada en el laboratorio bajo los factores de integridad, disponibilidad, confidencialidad y trazabilidad, excluyendo a criterio propio la autenticidad, pues este aspecto no es de relevancia para tener en cuenta en el análisis de riesgos ya que durante las actividades realizadas en la organización se conoce con exactitud quien hace uso de los datos y los servicios, por tanto esta dimensión se encuentra controlada y no afecta el desempeño de los procesos.

14.3.1 Pasos utilizados en el desarrollo de la matriz de riesgo del Laboratorio Clínico Patológico López Correa según la metodología Magerit 3.0.

1) Se hace un inventario de los activos, tipos de activos y clasificarlos por dependencia:

Tabla 10. Valoración de activos.

TIPO	NOMBRE DEL ACTIVO	VALOR				
		Integridad	Disponibilidad	Confidencialidad	Trazabilidad	TOTAL
DATOS / INFORMACION	usuarios / carpetas de red	4	3	2	4	**13**
	copias de respaldo: Data Base	4	4	2	5	**15**
	copias de respaldo: unidad de almacenamiento sede megacentro	4	4	2	5	**15**
	copias de respaldo: Información	4	4	2	5	**15**
	copias de respaldo: Información equipos clientes	4	4	2	5	**15**
	Datos de configuración: Manuales de procedimientos	2	2	3		**7**
	Registro de actividad: Formato de incidentes	1	1	2		**4**
SERVICIOS	Cobas C501	4	5	5	4	**18**
	Celldyn Ruby	4	5	5	4	**18**
	Inmulite	4	5	5	4	**18**
	Nanoduct	4	5	5	4	**18**
	AVL	4	5	5	4	**18**
	Cobas 601	4	5	5	4	**18**
	Cobas 701	4	5	5	4	**18**
	CS-2100i	4	5	5	4	**18**
	Alifax Test 1	4	5	5	4	**18**
	Vitek 2 compact / Bact – Alert 3D	4	5	5	4	**18**
	Tunderbolth	4	5	5	4	**18**
	DS2	4	5	5	4	**18**
	Genexpert	4	5	5	4	**18**
	VIPER	4	5	5	4	**18**
	Alinity	4	5	5	4	**18**

APLICACIONES	Winsislab	5	5	5	5	**20**
	Geminus	5	5	5	5	**20**
	Pagina WEB	4	3	5	2	**14**
	Cliente de correo electronico interno	3	2	2	2	**9**
	Herramientas de ofimatica	1	2			**3**
	Antivirus	4	4			**8**
	Sistema operativo	3	3		3	**9**
	Gestor de maquinas virtuales	4	4			**8**
	Sistema de backup	4	4		3	**11**
EQUIPAMIENTO INFORMATICO	Servidores	5	5	5	5	**20**
	Computadores	3	4	4	4	**15**
	Celulares	4	1	2	2	**9**
	Portatiles	3	4	5	4	**16**
	Informatica personal	1	1	1		**3**
	Impresoras	1	3			**4**
	Escaneres	1	3			**4**
	Dispositivos criptograficos: llaves - firmas digitales	5	2	5		**12**
	Routers	2	3			**5**
	Switch	4	4			**8**
	Cortafuegos - firewall	5	5	4		**14**
	punto de acceso inalambrico - red independiente	3	3		2	**8**
	planta telefonica	4	4			**8**
REDES DE COMUNICACIONES	ADSL	4	4			**8**
	Telefonia Movil	4	4			**8**
	Red Local	4	4		3	**11**
	Red metropolitana WAN	4	4	3		**11**
SOPORTE DE INFORMACION	Almacenamiento en red: NAS	4	4	4	4	**16**
	Material impreso	5	4	5	4	**18**
EQUIPAMIENTO AUXILIAR	Cableado Categoria 6 Red	3	4			**7**
	Cable electrico	5	4			**9**
	Suministros esenciales	4	4			**8**
	Gabinete - Rack	4	3			**7**
	Aire acondicionado	3	3			**6**
INSTALACIONES	Recinto : Edificio	5	5	4		**14**
	Cuarto de sistemas	5	5	5	4	**19**
PERSONAL	Usuarios Externos	3	3	4		**10**
	Usuarios Internos	4	4	4	4	**16**
	Administrador del Sistema, Comunicaciones, BBDD y Seguridad: Coordinador de Sistemas de Información y Tecnologia	4	4	4	4	**16**
	Desarrolladores / Programadores (winsilab - geminus)	4	4	4	4	**16**
	Proveedores	4	3	3		**10**

Fuente: Elaboración propia.

2) Se realiza la valoración de los activos de acuerdo con las dimensione de seguridad (Integridad, Disponibilidad, Confidencialidad y trazabilidad) teniendo en cuenta la siguiente escala de valoración:

Tabla 11. Escala de valores de activos.

ESCALA DE VALOR DE ACTIVOS		
Valor		**Criterio**
5	Muy alto	Daño muy grave a la organización
4	Alto	Daño grave a la organizació
3	Medio	Daño importante a la organización
2	Bajo	Daño menor a la organización
1	Despreciable	Irrelevalnte a efectos practicos
Fuente: EAR/LAR 5.4.5 Escala de valoración		

El valor del activo se calcula sumando los valores de los criterios dados en cada dimensión de seguridad.

3) Se desarrolla la Matriz Análisis de Riesgos descrita en el Anexo 4 – Matriz análisis de riesgos Magerit 3.0 de la siguiente manera:

A. Se identifica con una X en las dimensiones de seguridad (Integridad, Disponibilidad, Confidencialidad y trazabilidad) las cuales afecten cada activo y se totaliza.

B. Se le da un peso a cada grupo de amenaza: Porcentaje estimado de afectación de cada grupo de amenazas sobre los activos según un juicio de expertos de la siguiente manera:

20% = Desastres Naturales
30% = De origen industrial
30% = Errores y fallos no intencionados
20% = Ataques intencionados

C. Se identifican y se califican las amenazas que afectan a cada activo según la metodología Magerit 3.0 de acuerdo con los siguientes criterios:

Tabla 12. Exposición a la amenaza.

EXPOSICIÓN A LA AMENAZA
1 - Bajo
2 y 3 - Medio
4 - Alto

Fuente: Elaboración propia.

Cada grupo de amenaza se totaliza por medio de la suma de sus amenazas multiplicado por el peso porcentual de la amenaza.

D. Se calcula el valor de la amenaza de cada activo sumando los totales de cada grupo de amenaza y multiplicándolos por el total de la clasificación de las dimensiones como se identifica en la columna BR del Anexo 4 – Matriz análisis de riesgos Magerit 3.0

E. Se calcula la clasificación de la degradación por cada activo como se identifica en la columna BS del Anexo 4 – Matriz análisis de riesgos Magerit 3.0 según un juicio de expertos dado el siguiente criterio:

Calificación de degradación: [1 = Bajo; 2 = Medio; 3 = Alto; 4 = Muy alto]

F. Se calcula la degradación de cada activo multiplicando la calificación de degradación por el valor de la amenaza como se identifica en la columna BT del Anexo 4 – Matriz análisis de riesgos Magerit 3.0.

G. Se calcula la clasificación de la probabilidad de ocurrencia de cada activo como se identifica en la columna BU del Anexo 4 – Matriz análisis de riesgos Magerit 3.0 según el histórico de la organización y por medio de un juicio de expertos dado el siguiente criterio:

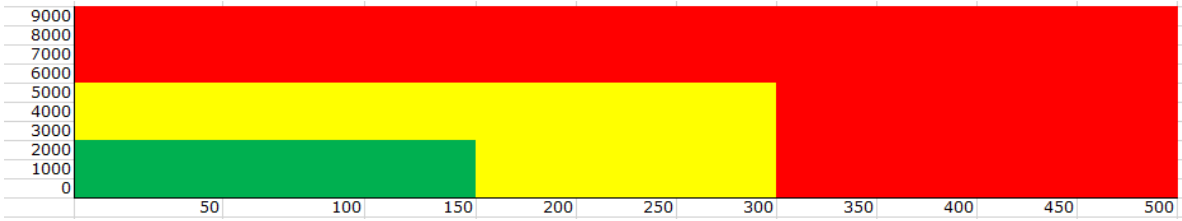
Calificación de probabilidad: [1 = Cada varios años; 2 = Una vez al año; 3 = Mensualmente; 4 = a diario]

H. Se calcula la probabilidad de cada activo multiplicando la clasificación de la probabilidad por la amenaza como se identifica en la columna BV Anexo 4 – Matriz análisis de riesgos Magerit 3.0.

I. Finalmente, se calcula el impacto de cada activo multiplicando el valor del activo por la degradación como se identifica en la columna BX del Anexo 4 – Matriz análisis de riesgos Magerit 3.0.

4) Se realiza el grafico de riesgo entre los valores calculados entre la probabilidad y el impacto con el fin de identificar los niveles del riesgo de cada activo según el siguiente mapa de calor:

Gráfico 3. Mapa de calor.



Fuente: Elaboración propia.

Tabla 13. Nivel de riesgo.

Nivel de Riesgo	Probabilidad	Impacto
Riesgo bajo	0-150	0-3000
Riesgo medio	151-300	3001-6000
Riesgo Alto	301-500	6001-9000

Fuente: Elaboración propia.

5) Basados en la metodología de Magerit 3.0 (Libro 2) se identifican las salvaguardas que actualmente se aplican en el laboratorio y se determinó por cada grupo de salvaguarda un porcentaje de reducción del riesgo como se muestra en la siguiente tabla:

Tabla 14. Salvaguarda.

SALVAGUARDA	% DE REDUCCIÓN DEL RIESG
Copias de seguridad (datos backup)	10%
Protección: Información, servicios, aplicaciones informaticas, equipos informaticos, comunicaciones, de la integridad de los datos intercambiados, Equipos Informáticos, central telefónica (PABX), de las Instalaciones, soportes de información, cableado.	20%
Se aplican perfiles de seguridad	10%
Gestión de cambios (mejoras y sustituciones)	5%
Cambios (actualizaciones y mantenimiento)	10%
Puesta en producción	5%
Aseguramiento de la disponibilidad	5%
Reproducción de documentos	5%
Autenticación del canal	10%
Limpieza de contenidos	5%
Destrucción de soportes	5%
Suministro eléctrico	10%
Instalación	10%
Climatización	5%
Diseño	10%
Control de los accesos físicos	10%
Control de acceso a usuario externo	10%
Acuerdos para intercambio de información y software	5%
Servicios: Adquisición o desarrollo	5%
Comunicaciones: Adquisición o contratación	5%

Fuente: Elaboración propia.

De acuerdo con cada tipo de salvaguarda los porcentajes de reducción del riesgo afectaran ya sea la probabilidad, el impacto o ambos según corresponda, recalculando nuevamente estos valores.

6) Se realiza de nuevo un gráfico de riesgo, pero en esta oportunidad afectado por las salvaguardas con el fin de identificar en un mapa de calor los niveles del riesgo actuales de cada activo.

Con esta información recolectada se realizan las recomendaciones pertinentes para reducir los niveles de riesgos altos y para prevenir que los niveles de riesgo medios aumenten.

14.3.2 Recomendaciones generales de acuerdo con el análisis de riesgos.

La principal recomendación administrativa que consideramos pertinente es implementar una planificación de seguridad, inspección de seguridad y gestión de riesgos para todos los activos con el fin de fortalecer el proceso de sistema de información del laboratorio.

PARA LOS RIESGOS ALTOS:

- La Categoría de Servicios es la que mayor afectación tuvo en el análisis de riesgos con todos sus activos en el nivel más alto de riesgo, convirtiéndose en la categoría más vulnerable y que requiere una mayor atención, por lo tanto, se recomienda implementar de manera general nuevas salvaguardas que permitan disminuir obligatoriamente el riesgo, las cuales podrían ser:

1) Gestionar Incidencias,
2) Desplegar herramientas de monitorización de tráfico,
3) Desarrollar herramientas de detección / prevención de intrusión.

Además, mejorar el soporte técnico de las casas comerciales con las cuales se tiene el riesgo compartido fortaleciendo los servicios proporcionados de la siguiente manera:

Tabla 15. Recomendaciones salvaguardas por activo.

ACTIVO	CASA COMERCIAL	RECOMENDACIÓN DE SALVAGUARDA
Cobas C501	Rochem	Gestión de vulnerabilidades y Generación de alertas
Celldyn Ruby	Abbott	Herramienta de chequeo de configuración
Inmulite	Siemens	Segregación de tareas
Nanoduct	Velez Lab	Verificar funciones de seguridad

AVL	Rochem	Gestión de vulnerabilidades y Generación de alertas
Cobas 601	Rochem	Gestión de vulnerabilidades y Generación de alertas
Cobas 701	Rochem	Gestión de vulnerabilidades y Generación de alertas
CS-2100i	Siemens	Segregación de tareas
Alifax Test 1	Velez Lab	Verificar funciones de seguridad
Vitek 2 compact / Bact – Alert 3D	Biomerieux	Gestión de vulnerabilidades
Tunderbolth	Annar Diagnostica	Control de acceso lógico
DS2	Annar Diagnostica	Control de acceso lógico
Genexpert	Rochem	Gestión de vulnerabilidades y Generación de alertas
VIPER	Becton Dickison	Gestión de vulnerabilidades
Alinity	Abbott	Herramienta de chequeo de configuración

Fuente: Elaboración propia.

- Para los Servidores (Categoría de Equipamento Informático) desarrollar una herramienta de detección / prevención de intrusión y una herramienta de gestión de análisis de vulnerabilidades.

PARA LOS RIESGOS MEDIOS:

Para prevenir que los activos que se encuentran en un nivel de riesgo medio pasen a un riesgo alto, se recomiendan implementar las siguientes salvaguardas:

- Para los activos Winsislab y Geminus (Categoría de Aplicaciones) desarrollar una herramienta de detección / prevención de intrusión y fortalecer la asistencia de los programadores y desarrolladores con el fin de mejorar la oportunidad en la entrega de las actualizaciones.

- Para el Almacenamiento en Red: NAS y el material impreso (Categoría Soporte de Información) Gestionar incidencias, realizar auditoria para verificar tiempos de retención, destrucción de documentos y digitalización total del material impreso.

- Para el Cuarto de Sistemas (Categoría Instalaciones) fortalecer el control de acceso físico ya existente e implementar una inspección de seguridad.

PARA LOS RIESGOS BAJOS:

Para los activos que se requiere consolidar en un nivel de riesgo bajo se recomienda desarrollar una herramienta de detección / prevención de intrusión.
Además, se resalta la buena aplicación de las siguientes salvaguardas que mantienen los activos en este nivel:

- ✓ Copias de seguridad (datos backup)
- ✓ Protección de los activos
- ✓ Aplicación de perfiles de seguridad
- ✓ Cambios (actualizaciones y mantenimiento)
- ✓ Aseguramiento de la disponibilidad

14.4 ELABORAR LA DOCUMENTACIÓN REQUERIDA EN LA FASE DE PLANEACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LOS REQUISITOS DE LA NORMA.

Como se muestra en la figura 6, los numerales 4 (alcance del SGSI), 5 (liderazgo), 6 (planificación) y 7 (soporte) corresponden al PLANEAR mientras que los numerales 8 (operación), 9 (evaluación del desempeño) y 10 (mejora) corresponden al HACER, VERIFICAR Y ACTUAR respectivamente, por lo tanto como el alcance de este proyecto es de la fase de planificación de la norma NTC/ISO/IEC 27001:2013 se desarrollaron únicamente los numerales del 4 al 7.

Figura 6. Estructura alineada a anexo SL.

Fuente: Elaboración propia

4 - CONTEXTO DE LA ORGANIZACIÓN.

4.1 - CONOCIMIENTOS DE LA ORGANIZACIÓN Y SU CONTEXTO.

El contexto del Sistema de Gestión de la Seguridad de la Información se describe en el Anexo 5 – DOFA SGSI.

4.2 - COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS.

El laboratorio reconoce a sus partes interesadas a:

Tabla 16. Partes interesadas.

PARTE INTERESADA	REQUISITO	REQUISITO DE OBLIGATORIO CUMPLIMIENTO Y REGLAMENTACIÓN	OBLIGACIONES CONTRACTUALES	NECESIDADES Y EXPECTATIVAS FRENTE A SEGURIDAD DE LA INFORMACION
Entes gubernamentales	*Cumplimiento con la legislación vigente.	*Protección de Datos Personales. *Políticas Laborales y Prestación de Servicios por Terceros. *Servicios de Comercio Electrónico. *Propiedad Intelectual.	*No aplica	Las partes interesadas esperan del Laboratorio Clínico Patológico López Correa un manejo responsable y adecuado de toda información. Adicionalmente estas partes interesadas tienen la convicción de que a través de la implementación, mantenimiento y mejora continua del SGSI la organización garantizará la integridad, disponibilidad, confidencialidad y trazabilidad de la información, Además del obligatorio cumplimiento de los requisitos legales, reglamentarios y contractuales vigentes.
Cliente	*Protección de resultados y control de calidad.	*Protección de datos personales. *NTC/ISO/IEC 27001:2013: confidencialidad, integridad, disponibilidad y trazabilidad.	*Confidencialidad	
Empleados	*Protección y manejo adecuado de la información personal.	*Protección de datos personales.	*Cláusulas de confidencialidad en los contratos	
Alta Dirección	*Continuidad del negocio.	*Certificado de cámara y comercio. *Plan de contingencia.	*No aplica	
Proveedores	*Uso adecuado de la información de los proveedores.	*Protección de datos personales.	*Cláusulas de confidencialidad en los contratos.	
Contratistas	*Controlar planilla de pago de seguridad social.	*Protección de datos personales.	*Seguridad de la información. *Cláusulas de confidencialidad en los contratos.	

Sistema de Gestión Integral (SGI)	*Confidencialidad *Disponibilidad *Integridad *Trazabilidad	*Norma NTC/ISO/IEC 27001:2013. *Norma ISO 9001:2015.	*Contratos.	

Fuente: Elaboración Propia.

4.3 - ALCANCE DEL SGSI

El Sistema de Gestión de la Seguridad de la Información de Laboratorio Clínico Patológico López Correa S.A., es aplicable a todos los procesos de la organización definidos en el Mapa de Procesos de la Institución en la Sede Centro ubicada en la Calle 24 No. 05-41.

4.4 - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El Laboratorio Clínico Patológico López Correa establece, implementa, mantiene y mejora continuamente el Sistema de Gestión de la Seguridad de la Información de acuerdos con los requisitos de la norma NTC/ISO/IEC 27001:2013.

5 - LIDERAZGO

5.1 - LIDERAZGO Y COMPROMISO

La alta dirección de Laboratorio Clínico patológico López Correa está conformada por: Gerente, Directora de Laboratorio, Directora Administrativa.
La Gerencia participa en la toma de decisiones y análisis de resultados presentados en la rendición de cuentas, todo enfocado al mejoramiento continuo.
La Política para la Seguridad de la Información está alineada con la planeación estratégica y objetivos de la Seguridad de la Información.

Los controles se construyen bajo el esquema Planear- Hacer- Verificar- Actuar, la evaluación de resultados se realiza en espacios como el Comité de Calidad, para asegurar que cuenten con los recursos necesarios, anualmente se genera el

presupuesto por sedes, el cual se elabora teniendo en cuenta la información del año anterior y para los ingresos se aplica un porcentaje según el crecimiento en ventas establecido por el área comercial y para los costos y gastos se le aplica el porcentaje de participación sobre las ventas.

El Comité de Calidad de Laboratorio Clínico patológico López Correa, establece su compromiso con el desarrollo de la implementación del Sistema Integrado de Gestión, así como la mejora continua de su eficacia.

5.2 - POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN

El Laboratorio Clínico Patológico López Correa dedicado a la prestación servicios de laboratorio clínico, patología, citología, toma de muestras de laboratorio clínico, toma de muestras de cuello uterino y ginecológicas, seguridad y salud en el trabajo busca por medio de la implementación de la NTC/ISO/IEC 27001:2013 garantizar la confidencialidad, disponibilidad, integridad y trazabilidad de la información, por medio de la implementación de controles que salvaguarden la información a través del seguimiento y monitoreo de la matriz de riesgos.

La organización se compromete con el mejoramiento continuo, el logro de los objetivos de la seguridad de la información y el cumplimiento de los requisitos legales y reglamentarios. Además, brinda a todos los colaboradores las herramientas necesarias para el cumplimiento de los lineamientos de la seguridad de la información y el cumplimiento de los requisitos de la norma.

- Política para dispositivos móviles**:**

El laboratorio establece las condiciones óptimas para el adecuado manejo y uso responsable por parte de los empleados y contratistas de los dispositivos móviles institucionales y/o personales tales como computadores portátiles, celulares, tabletas, entre otros, que tienen acceso a la información del laboratorio, implementando controles de acceso, copias de seguridad y demás elementos que se consideren necesarios para garantizar la seguridad de la información.

- Política para el Teletrabajo:

El laboratorio garantiza la confidencialidad, integridad, disponibilidad y trazabilidad de la información utilizada a través del Teletrabajo para todos los empleados y contratistas brindándoles los recursos necesarios para realizar su labor

remotamente de acuerdo con lo establecido en la normatividad legal aplicable y vigente, cumpliendo con el protocolo de asignación de recursos y monitoreo de actividades de los teletrabajadores.

- Política de Control de Acceso:

El laboratorio garantiza la protección contra cualquier tipo acceso (digital y/o físico) no autorizado de la información, de las áreas de procesamiento de la información, de las redes de datos, de los servicios en red, de los recursos de la plataforma tecnológica y del servicio de información por medio de controles de acceso idóneos. Se limita y se restringe el acceso a empleados y/o contratistas de la información sensible garantizando la confidencialidad e integridad de esta.

- Política de Escritorio Limpio y Pantalla Limpia:

El laboratorio previene la perdida, el daño y/o el acceso no autorizado de la información contenida en los puestos de trabajo, computadores, escáner, impresoras, dispositivos móviles y medios magnéticos usados por empleados y/o contratistas mediante el cumplimiento de lineamientos de escritorio y pantalla limpia que permitan proteger los documentos en papel y dispositivos de almacenamiento removibles susceptibles.

- Política de Transferencia de Información:

El laboratorio protege el intercambio de información alojada en cualquier medio electrónico (servidores, puestos de trabajo, medios de almacenamiento removibles, entre otros.) o físico (Carpetas, libros, formatos, registros, entre otros.), que requiera ser transferida entre colaboradores, contratistas y/o partes interesadas, siendo protegidas bajo todos los niveles de integridad y confidencialidad, contando con la autorización pertinente para el tratamiento de datos.

- Política de Desarrollo Seguro:

El laboratorio vigila y realiza seguimiento al desarrollo seguro y mantenimiento de todo software tanto interno como externo, estableciendo criterios de seguridad considerados en todas las etapas tanto de desarrollos, actualizaciones e instalaciones de software.

- Política de Seguridad de la Información para las relaciones con los Proveedores:

El laboratorio garantiza la protección de los activos a los que tienen acceso los proveedores, manteniendo un nivel óptimo de seguridad de la información y de la entrega del servicio, alineados con los acuerdos establecidos entre las partes.

5.3 - ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

Los roles, responsabilidades y autoridades pertinentes a la Seguridad de la Información se encuentran definidos en el Anexo 6 – Funciones, Responsabilidades y Autoridades del SGSI.

6 - PLANIFICACIÓN

6.1 - ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

El Laboratorio Clínico Patológico López Correa implementa acciones necesarias para tratar los riesgos y oportunidades por medio del desarrollo de una metodología de gestión del riesgo llamada Magerit 3.0, en la cual se realizó un análisis de gestión de riesgos por medio de una matriz comprendida en el Anexo 4 – Matriz análisis de riesgos Magerit 3.0 en donde se aplicó:

La valoración del riesgo de la seguridad de la información de acuerdo con la integridad, disponibilidad, confiabilidad y trazabilidad de la información.

El tratamiento de riesgos de la seguridad de la información, por medio de la aplicación de controles que reducen, comparten y/o aceptan el riesgo, salvaguardando la información de posibles daños o perdidas. Adicional se produjo una declaración de aplicabilidad Anexo 7 – Declaración de aplicabilidad.

6.2 - OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

- Asegurar el compromiso de la Alta Dirección con el Sistema de Gestión de Seguridad de la Información.

- Determinar los controles adecuados que permitan definir un plan de tratamiento de los riesgos que garanticen que se mantengan en un nivel aceptable de riesgo.
- Proteger los activos de la información con base en los criterios de confidencialidad, integridad, trazabilidad y disponibilidad.

- Garantizar el cumplimiento de los requerimientos legales, reglamentarios y contractuales vigentes.

- Capacitar y sensibilizar al personal del laboratorio y partes interesadas sobre el SGSI fortaleciendo el nivel de conciencia, creando una cultura de seguridad.

- Garantizar la continuidad de los servicios prestados por el laboratorio.

- Implementar acciones correctivas y de mejora para el SGSI que permitan alcanzar niveles más avanzados de seguridad de la información.

7 - SOPORTE

7.1 - RECURSOS

El Laboratorio Clínico Patológico López Correa desde la Alta Dirección, garantiza la asignación de los recursos necesarios para planificar, implementar, mantener y mejorar continuamente el Sistema de Gestión de la Seguridad de la Información.

7.2 - COMPETENCIA

Las competencias necesarias para que el personal ejecute las actividades que aseguran la eficacia del Sistema de Gestión de la Seguridad de la Información se encuentra documentada en la descripción de cargo en el Anexo 8 - Descripción de cargos. La gestión por competencias se realiza según lo definido en el programa de gestión por competencias liderado desde el proceso de Gestión Gerencial y Talento Humano.

Se cuenta con el manual de procedimientos de Talento Humano que contiene las actividades de inducción, entrenamiento y reentrenamiento del personal descrito en el Anexo 9 - Manual de procedimientos selección y mejoramiento de talento humano v10.

7.3 -TOMA DE CONCIENCIA

En el Laboratorio Clínico Patológico López Correa se desarrollan las siguientes actividades que fortalecen la toma de conciencia de toda la institución:

Reuniones de procesos, seguimiento al desempeño a través de indicadores, aplicación de listas de chequeo, encuesta del contexto interno, capacitaciones, intervenciones de los comités institucionales, seguimiento a través de la revisión por la Dirección, socialización de las responsabilidades y autoridades de cada cargo, socialización de las políticas del Sistema Integrado de Gestión.

7.4 – COMUNICACIÓN

El Laboratorio Clínico Patológico López Correa documenta en la Matriz de Comunicaciones comprendida en el Anexo 10 - Matriz de comunicación v3 de acuerdo con las necesidades de tener comunicaciones internas y externas pertinentes al Sistema de Gestión de la Seguridad de la Información.

7.5 - INFORMACIÓN DOCUMENTADA

De acuerdo con alcance de este proyecto se elaboró la documentación requerida por la norma y por la organización en la fase de planificación.

El Laboratorio Clínico Patológico López Correa tiene implementado un procedimiento de información documentada Anexo 11 – Información documentada v2 con el objetivo de asegurar el control de la información y la eficacia del Sistema Integrado de Gestión.

15 RESULTADOS: ANALISIS Y DISCUCIÓN

En la elaboración del proyecto se desarrollaron las siguientes actividades:

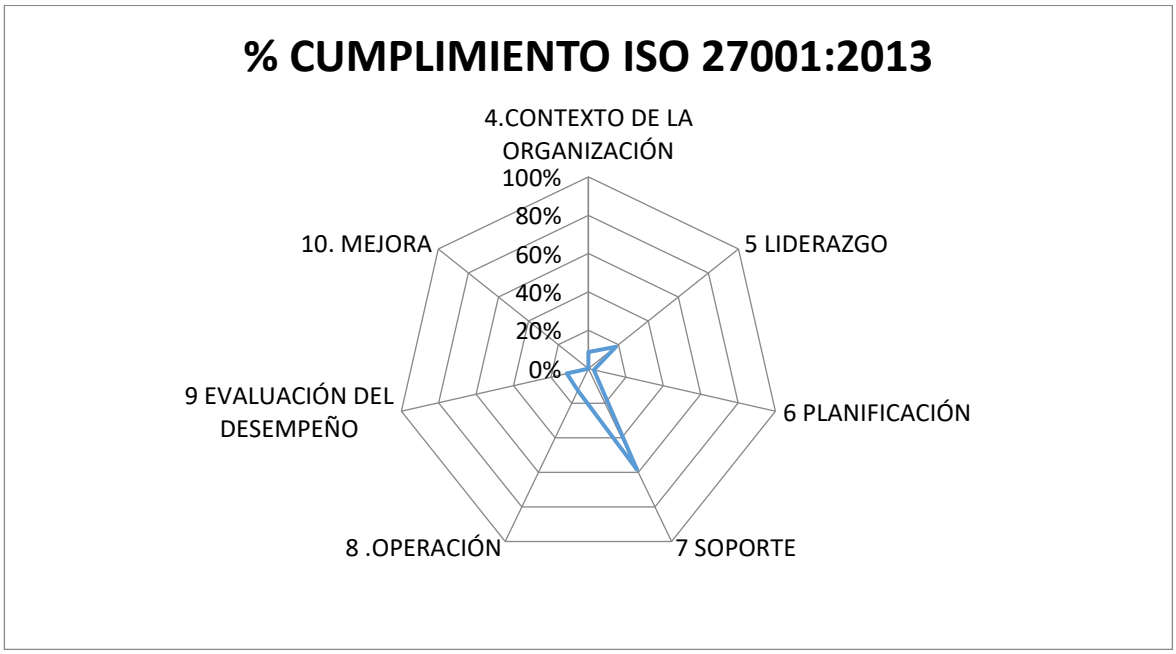
Se diseño e implementó una herramienta diagnostico para desarrollar el análisis del servicio de información. Posteriormente se consolidaron los resultados y se realizó un comparativo con el diagnostico actual frente a los requisitos norma NTC/ISO/IEC 27001:2013 y el anexo A, identificando las diferencias y faltantes del servicio de información del laboratorio y se realizó un análisis por cada numeral. Consecutivamente se identificó la metodología de gestión del riesgo adecuada para el laboratorio mediante un análisis comparativo de ventajas y desventajas entre cinco metodologías seleccionadas y se implementó la metodología Magerit 3.0 en el sistema de la información del laboratorio a través de la matriz de riesgos.

Se elaboro una matriz de controles basados en el anexo A de la norma NTC/ISO/IEC 27001:2013 y se identificaron las fases de PHVA, haciendo un análisis y recomendaciones de cumplimiento de la fase de planear. Adicional se identificó y se elaboró la documentación necesaria en la fase de planeación para darle cumplimiento a los requisitos de la norma.

Los resultados alcanzados en este proyecto se muestran a continuación:

En los resultados obtenidos de la aplicación de la herramienta diagnóstico frente a los numerales de la norma NTC/ISO/IEC 27001:2013 se calculó el porcentaje total de cumplimiento de adecuación siendo del **16%**. En donde el numeral 7 Soporte alcanzó el mayor porcentaje de 58% mientras que los numerales 6 Planificación y 10 Mejora alcanzaron un porcentaje 3% y 0% respectivamente catalogándose como los numerales de menor cumplimiento y los cuales requerirán una mayor atención.

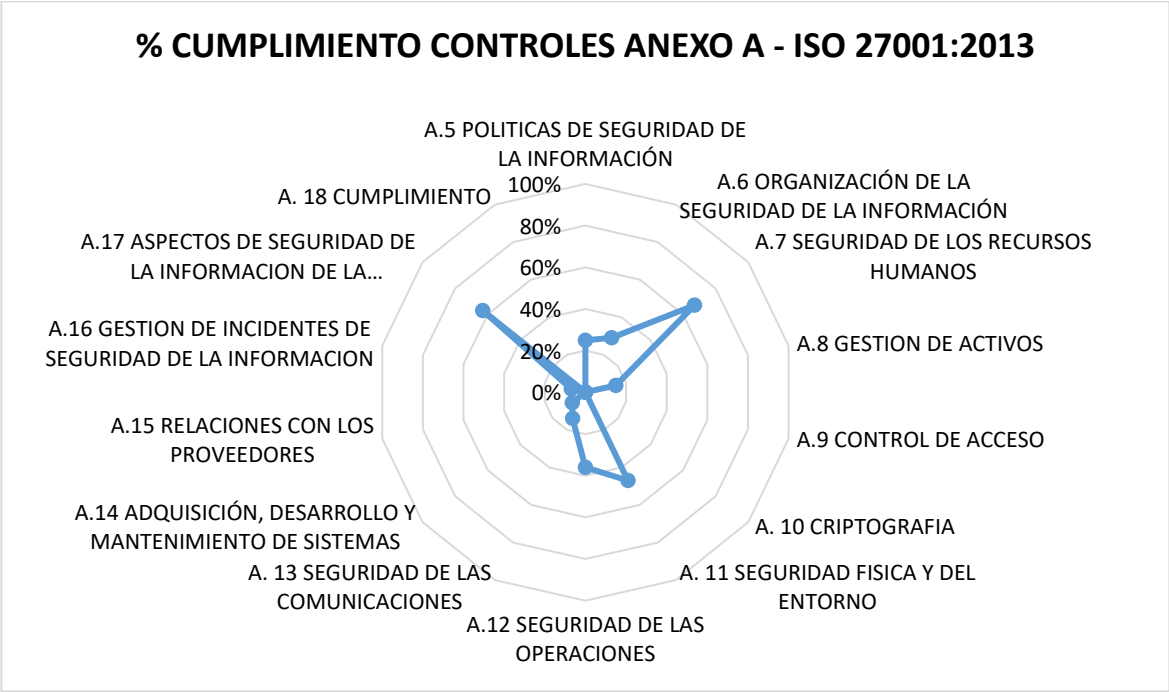
Gráfico 4. Porcentaje de cumplimiento ISO 27001.



Fuente: Elaboración propia.

En los resultados obtenidos de la aplicación de la herramienta diagnóstico frente al anexo A de la norma NTC/ISO/IEC 27001:2013 se calculó el porcentaje total de cumplimiento de adecuación siendo del **22%**. En donde el control A7 Seguridad de los Recursos Humanos y el control A17 Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio alcanzaron el mayor porcentaje de 67% y 63% respectivamente mientras que los controles A9 Control de Acceso, A10 Criptografía, A15 Relaciones con los Proveedores y A18 Cumplimiento, alcanzaron un porcentaje del 0% catalogándose como los anexos sin ningún tipo de control y los cuales requerirán una mayor atención.

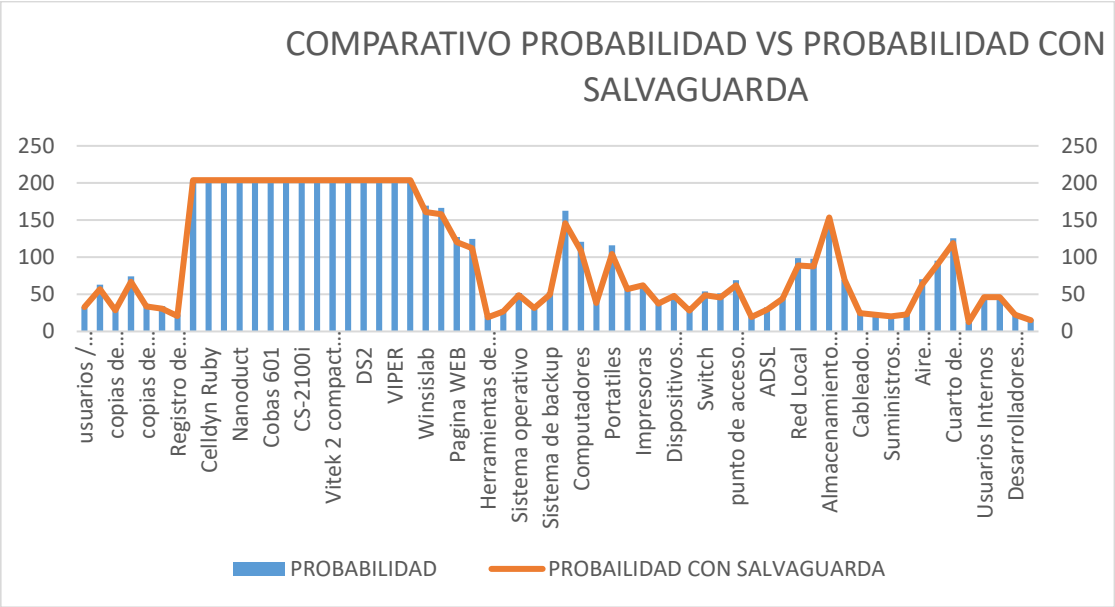
Gráfico 5. Porcentaje de cumplimiento anexo A.



Fuente: Elaboración propia.

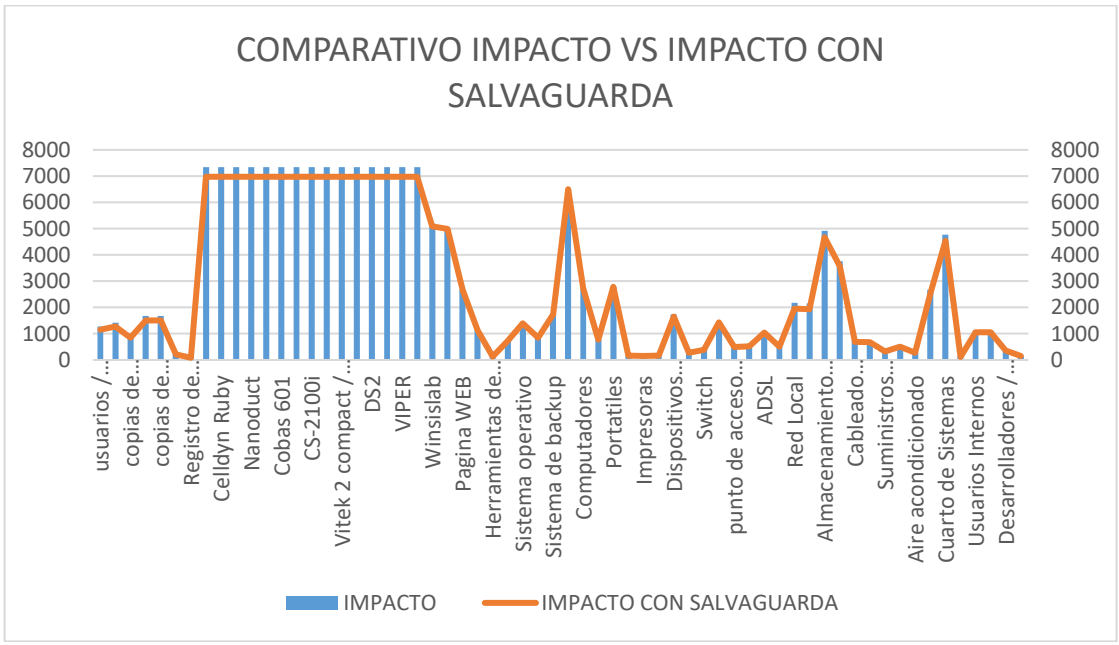
En el desarrollo de la metodología de gestión del riesgo de MAGERIT 3.0, con la matriz de análisis de riesgos y aplicación de controles, se puede observar en los siguientes gráficos la disminución de la probabilidad y el impacto de amenazas en cada activo, contando con las salvaguardas adecuadas.

Gráfico 6. Comparativo probabilidad vs probabilidad con salvaguarda.



Fuente: Elaboración propia.

Gráfico 7. Comparativo impacto vs impacto con salvaguarda.



Fuente: Elaboración propia.

De acuerdo con el alcance del proyecto, según los requisitos de la norma NTC/ISO/IEC 27001:2013 se documentaron los numerales 4 (alcance del SGSI) ,5 (liderazgo), 6 (planificación) y 7 (soporte) que corresponden a la fase de Planeación del Sistema de Gestión de la Seguridad de la Información SGSI, dejando como recomendación a la organización ampliar el alcance a las fases hacer, verificar y actuar para así culminar con la documentación del sistema de gestión dándole cumplimiento a todos los requisitos de los numerales 8 (operación), 9 (evaluación del desempeño) y 10 (mejora) de la norma NTC/ISO/IEC 27001:2013

Se concluye que los resultados y análisis obtenidos en la elaboración de este proyecto dieron cumplimiento a los objetivos específicos y así mismo al propósito del objetivo general.

16 CONCLUSIONES

Durante el desarrollo de este proyecto en el cual se dio cumplimiento al objetivo general documentando el Sistema de Gestión de la Seguridad de la Información del Laboratorio Clínico Patológico López Correa S.A. bajo los requisitos de la Norma NTC/ISO/IEC 27001:2013 se llegaron a ciertas conclusiones descritas a continuación:

1) Contar con un Sistema de Gestión de la Seguridad de la Información crea un alto prestigio y reputación de la organización frente a sus usuarios y sus clientes ya que en el laboratorio se maneja información sensible y confidencial la cual requiere una garantía de seguridad.

2) Realizar el análisis diagnóstico del estado actual de la norma NTC/ISO/IEC 27001:2013 y del anexo A frente a la seguridad de la información del Laboratorio Clínico Patológico López Correa e identificar las diferencias entre el servicio actual y los requisitos de la norma, permitió evidenciar claramente las mejoras que se requieren implementar de acuerdo con los controles necesarios para asegurar la integridad, disponibilidad, confiabilidad y trazabilidad de la información, siendo una avance importante para la adecuada implementación del sistema de gestión de la seguridad de la información de la organización.

3) Realizar la valoración de los activos permitió comprenderlos y estimarlos adecuadamente, ya que por medio de la medición cuantitativa del nivel de criticidad se tiene una mayor certeza de que tan expuestos están los activos y así tener mayor atención a estos.

4) Elegir a Magerit 3.0 como la metodología de análisis de riesgos fue una decisión acertada ya que por medio de la matriz y los gráficos de riesgos se nos brindó un panorama claro sobre las amenazas y vulnerabilidades en las que se encuentra expuesto la empresa y sus probabilidades e impactos de ocurrencia, y como por medio de las salvaguardas estos riesgos se mitigan, se comparten o se aceptan dándole un adecuado tratamiento por medio de controles eficientes y seguros.

5) En la documentación de la norma NTC/ISO/IEC 27001:2013 en la fase de planeación se determinaron las políticas, procedimientos y documentos adecuados para el óptimo desarrollo del Sistema de Gestión de la Seguridad de la Información en donde por medio de estos se garantiza la integridad, disponibilidad, confidencialidad y trazabilidad de la información del Laboratorio Clínico Patológico López Correa.

6) Finalmente, el desarrollo de este proyecto es el primer paso de muchos que quedan pendientes por dar en una organización que está comprometida con el mejoramiento continuo y la cultura de cambio de la seguridad de la información.

17 RECOMENDACIONES

Así mismo se describen a continuación una serie de recomendaciones a tener en cuenta por el Laboratorio Clínico Patológico López Correa S.A. para que pueda culminar exitosamente la implementación y mantenimiento de su Sistema de Gestión de la Seguridad de la Información.

1) Continuar con la etapa de documentación del Sistema de Gestión de la Seguridad de la Información basados en la norma NTC/ISO/IEC 27001:2013 en las fases siguientes de hacer, verificar y actuar y si la Alta Dirección lo considera pertinente certificarse en esta norma.

2) Fortalecer la cultura de la seguridad de la información a todos los usuarios internos y externos de la organización a través de capacitaciones y toma de conciencia, por medio de jornadas de sensibilización para aplicar buenas prácticas de las políticas de seguridad y crear hábitos de seguridad, como bloquear sesiones en periodos de inactividad laboral, cambiar periódicamente sus contraseñas.

3) Ampliar el alcance del Sistema de Gestión de la Seguridad de la Información a todas las demás sedes del Laboratorio Clínico Patológico López Correa.

4) En caso de cambiar los activos o de mejorar la tecnología de información se debe actualizar la matriz de riesgos.

5) Fortalecer las salvaguardas de los activos que se identificaron como más críticos para reducir el nivel de riesgo.

6) Revisar periódicamente los controles basados en el anexo A de la norma NTC/ISO/IEC 27001:2013 para asegurar su adecuada implementación en el laboratorio.

18 REFERENCIAS BIBLIOGRÁFICAS

1. A, Martha Isabel Ladino, Paula Andrea Villa S, y Ana María López E. «Fundamentos De Iso 27001 Y Su Aplicación En Las Empresas». *Scientia Et Technica* XVII, n.º 47 (2011): 334-39. https://www.redalyc.org/articulo.oa?id=84921327061.
2. Abrego Almazán, Demian, José Melchor Medina Quintero, Mónica Lorena Sánchez Limón, Demian Abrego Almazán, José Melchor Medina Quintero, y Mónica Lorena Sánchez Limón. «Los Sistemas de Información en el Desempeño Organizacional: Un Marco de Factores Relevantes». *Investigación administrativa* 44, n.º 115 (junio de 2015): 0-0. http://www.scielo.org.mx/scielo.php?script=sci_abstract&pid=S2448-76782015000100001&lng=es&nrm=iso&tlng=es.
3. Álvarez, Vasco Rodrigo Talavera. «DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD ESTATAL DE SALUD DE ACUERDO A LA ISO/IEC 27001:2013», s. f., 90.
4. Armendáriz, Diana Nathaly López. «Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000», s. f., 19.
5. Burgos, Oscar Duarte, y Mario Roberto Monges Olmedo. «Análisis de una metodología de Seguridad de la Información basados en los estándares ISO 27001». *Revista ScientiAmericana* 5, n.º 2 (12 de noviembre de 2018). http://www.uamericana.edu.py/revistacientifica/index.php/scientiamericana/article/view/271.
6. Crespo-Martínez, Esteban, y Geovanna Cordero-Torres. «ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES». *UDAAKADEM*, n.º 1

(2016): 38-47. http://revistas.uazuay.edu.ec/index.php/udaakadem/article/view/129.
7. Cruz-Gavilánez, Yolanda de la N., y Carlos J. Martínez-Santander. «ISO / IEC 27001 aseguramiento de la calidad de la información: Línea de tiempo», 2018. https://doi.org/10.23857/pc.v3i6.641.
8. «Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013». Accedido 4 de marzo de 2020. http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6045.
9. «Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013». Accedido 4 de marzo de 2020. http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6092.
10. «Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos.» Accedido 4 de marzo de 2020. http://www.repositorioacademico.usmp.edu.pe/handle/usmp/609.
11. Flores, Victor Miguel Baca. «DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL - CHICLAYO». *INGENIERÍA: Ciencia, Tecnología e Innovación* 3, n.º 1 (12 de julio de 2016): 42-57. http://revistas.uss.edu.pe/index.php/ING/article/view/357.
12. «Gobierno de seguridad de la información, un enfoque hacia el cumplimiento regulatorio | Ochoa Arevalo | Revista Tecnológica - ESPOL». Accedido 13 de febrero de 2020. http://rte.espol.edu.ec/index.php/tecnologica/article/view/373/258.
13. Gómez, Carlos, Francisco Valencia, Carlos Marulanda, Carlos Gómez, Francisco Valencia, y Carlos Marulanda. «Las Tecnologías de la Información y las Comunicaciones y los Servicios Tecnológicos en las Entidades Públicas del Triángulo del Café en Colombia». *Información tecnológica* 29, n.º 4 (agosto de 2018): 119-26. https://doi.org/10.4067/S0718-07642018000400119.
14. Gómez, Enrique Ferruzola, Johanna Duchimaza S, Johanna Ramos Holguín, y María Alejandro Lindao. «Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT». *Revista Científica y Tecnológica UPSE* 6, n.º 1 (21 de junio de 2019): 34-41. https://doi.org/10.26423/rctu.v6i1.429.
15. Guamán, Carlos Roberto Sampedro, Silvio Amable Machuca Vivar, Diego Paúl Palma Rivera, Frankz Alberto, y Carrera Calderón. «PERCEPCIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS EN SANTO DOMINGO», s. f., 8.
16. Martelo, Raúl J., Jhonny E. Madera, y Andrés D. Betín. «Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)». *Información tecnológica* 26, n.º 2 (2015): 129-34. https://doi.org/10.4067/S0718-07642015000200015.
17. Martínez, Esteban Crespo, y Esteban Crespo Martínez. «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs». *Enfoque UTE* 8 (febrero de 2017): 107-21. https://doi.org/10.29019/enfoqueute.v8n1.140.

18. Mesquida, Antoni Lluís, Antonia Mas, Tomás San Feliu, y Magdalena Arcilla. «Integración de Estándares de Gestión de TI mediante MIN-ITs». *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º SPE1 (marzo de 2014): 31-45. https://doi.org/10.4304/risti.e1.31-45.
19. Monsalve-Pulido, Julián Alberto, Fredy Andrés Aponte-Novoa, y David Fernando Chaves-Tamayo. «Information Vulnerabilities' Study and Management, for a Private Enterprise in the Boyacá Colombian Department». *Revista Facultad de Ingeniería* 23, n.º 37 (julio de 2014): 65-72. http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S0121-11292014000200007&lng=en&nrm=iso&tlng=es.
20. Montenegro, Fabio Adalberto Arellano. «REALIZAR EL ANÁLISIS PARA GESTIÓN DE RIESGOS EN LOS SISTEMAS DE INFORMACIÓN DE LA IPS SOLIDARIOS SALUD DEL MUNICIPIO DE CUASPUD CARLOSAMA A PARTIR DE LA NORMA ISO 27001 APLICANDO LA METODOLOGÍA MAGERIT», 2018, 176.
21. Muñoz, Ararat, y Johanna Carolina. «Diseño de un SGSI basado en la Norma ISO 27001 para la empresa MA PEÑALOSA CÍA. S.A.S. sede principal Cúcuta.», 4 de noviembre de 2018. http://repository.unad.edu.co/handle/10596/21259.
22. Murillo, Navira Gissela Angulo, María Fernanda Zambrano Vera, Gabriel García Murillo, y Francisco Bolaños- Burgos. «PROPUESTA METODOLÓGICA DE SEGURIDAD DE INFORMACIÓN PARA PROVEEDORES DE SERVICIOS DE INTERNET EN ECUADOR». *Mikarimin. Revista Científica Multidisciplinaria. e-ISSN 2528-7842* 4, n.º 4 (28 de septiembre de 2018): 165-76. http://45.238.216.13/ojs/index.php/mikarimin/article/view/1197.
23. Parada, Diego J., Angélica Flórez, Urbano E. Gómez, Diego J. Parada, Angélica Flórez, y Urbano E. Gómez. «Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas». *Información tecnológica* 29, n.º 1 (febrero de 2018): 27-38. https://doi.org/10.4067/S0718-07642018000100027.
24. Salazar, Jorge Burgos, y Pedro G Campos. «Modelo Para Seguridad de la Información en TIC», s. f., 20.
25. «Modelo Para Seguridad de la Información en TIC», s. f., 20.
26. «Sistema de gestión de seguridad de la información en la municipalidad distrital de pira aplicando la norma iso/iec 27001:2013». Accedido 2 de marzo de 2020. http://repositorio.uladech.edu.pe/handle/123456789/11988.
27. Tenesaca, Campaña, y Óscar Eduardo. «Plan de propuesta para la implementación de la norma de seguridad informática ISO 27001 2005, para el Grupo Social Fondo Ecuatoriano Populorum Progressio (GSFEPP)», noviembre de 2010. http://dspace.ups.edu.ec/handle/123456789/4468.
28. Valencia-Duque, Francisco Javier, y Mauricio Orozco-Alzate. «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000». *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º 22 (junio de 2017): 73-88. https://doi.org/10.17013/risti.22.73-88.

29. «Vista de Metodologías para el análisis de riesgos en los sgsi | Publicaciones e Investigación». Accedido 3 de abril de 2020. https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754.
30. Yagual, Ricardo Rafael Coello, y Lucia Magdalena Pico Versoza. «Análisis de las ventajas y desventajas del sistema de gestión dela seguridad de la información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data en el Ecuador». *INNOVA Research Journal*, 4 de abril de 2018, 181-95. https://doi.org/10.33890/innova.v3.n4.2018.562.
31. Yupanqui, Josue Ruben Altamirano, y Sussy Bayona Oré. «Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento». *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º 25 (diciembre de 2017): 112-34. https://doi.org/10.17013/risti.25.112-134.
32. Norma Técnica Colombiana NTC-ISO-IEC 2001, ICONTEC, 2013-12-11, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.

33. Guía Técnica Colombiana GTC-ISO/IEC 27002, ICONTEC, 2015-07-22, Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

34. MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro l - Método. Madrid, octubre de 2012.

35. MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro ll - Catálogo de elementos. Madrid, octubre de 2012.

36. MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro lll - Guía de técnicas. Madrid, octubre de 2012.